ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

HENRIQUE RIBEIRO DA ROCHA

GOVERNANÇA SECURITÁRIA DO CIBERESPAÇO:
QUESTÕES SOBRE SEGURANÇA E DEFESA

Rio de Janeiro
2022

HENRIQUE RIBEIRO DA ROCHA

GOVERNANÇA SECURITÁRIA DO CIBERESPAÇO:

QUESTÕES SOBRE SEGURANÇA E DEFESA

Texto apresentado como Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares

Orientador: Prof. Dr. Luiz Rogério Franco Goldoni

Rio de Janeiro
2022

R672g Rocha, Henrique Ribeiro da.

Governança Securitária do Ciberespaço: questões sobre Segurança e Defesa. / Henrique Ribeiro da Rocha. —2021.

122 f. : il. ; 30 cm

Orientação: Luiz Rogério Franco Goldoni**.**

Dissertação (Mestrado em Ciências Militares)—Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.

Bibliografia: f. 109-120

1. CIBERESPAÇO. 2. GOVERNANÇA SECURITÁRIA DO CIBERESPAÇO. 3. DEFESA CIBERNÉTICA. 4. SEGURANÇA CIBERNÉTICA. 5. ESTADOS UNIDOS. 6. REINO UNIDO. I. Título.

CDD 003.5

HENRIQUE RIBEIRO DA ROCHA

GOVERNANÇA SECURITÁRIA DO CIBERESPAÇO: QUESTÕES SOBRE SEGURANÇA E DEFESA

Dissertação apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Mestre em Ciências Militares.

Aprovada em 31 de janeiro de 2022.

BANCA EXAMINADORA

LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Presidente
Escola de Comando e Estado-Maior do Exército - ECEME

KARINA FURTADO RODRIGUES – Profª Drª – Membro
Escola de Comando e Estado-Maior do Exército - ECEME

Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 07/02/2022 09:12:15-0300
CPF: 291.367.488-70
Verifique as assinaturas em https://v.ufsc.br

DANIELLE JACON AYRES PINTO – Membro
Universidade Federal de Santa Catarina - UFSC

Ciente

HENRIQUE RIBEIRO DA ROCHA – Postulante
Escola de Comando e Estado-Maior do Exército

Dedico esta dissertação aos meus pais.

AGRADECIMENTOS

Ao meu orientador, Professor Luiz Rogério Franco Goldoni, sempre disposto a me guiar, por estar presente em cada etapa de minha pesquisa, bem como por contribuir com ótimos conselhos e sugestões. Em um cenário tão instável como foi o período no qual esta dissertação foi escrita, especialmente devido a pandemia de COVID-19, você representou estabilidade e constância, o que me permitiu trabalhar da melhor forma possível.

Aos meus pais, e a minha irmã, cujo apoio e amor incondicionais são o que me mantém firme na busca de meus objetivos acadêmicos e pessoais desde que saí de casa para estudar. Vocês são o meu mundo.

As minhas amigas e aos meus amigos, que agora se encontram espalhadas e espalhados pelo Brasil e pelo mundo. Mas que ao mesmo tempo estão sempre presentes em minha caminhada, fornecendo apoio, amor, conselhos e, até mesmo, ideias de pesquisa!

À minha incrível banca de avaliação, composta pelas Professoras Danielle Jacon Ayres Pinto e Karina Furtado Rodrigues, que representam dois dos meus maiores exemplos sobre o que significa ser professor(a) e pesquisador(a) no Brasil, pelos apontamentos e sugestões para tornar o meu trabalho melhor.

Ao Pró-Defesa IV - Ciência, Tecnologia e Inovação em Defesa Cibernética e Defesa Nacional -, pelo apoio e fomento à minha pesquisa, o que permitiu que eu saísse do Sul do Brasil para realizar meu trabalho no Rio de Janeiro. Aproveito para agradecer, também, à rede de pesquisadores envolvidos no projeto.

Por fim, agradeço à Escola de Comando e Estado-Maior do Exército, que foi minha casa ao longo dos últimos dois anos, e ao excelente corpo docente e técnico-administrativo do Instituto Meira Mattos.

"*The march of technology and progress guarantees that even while we debate this definition—regardless of exactly how we define it now and refine it in the future—our use of cyberspace has already reached the point where an increasingly wide range of social, political, economic, and military activities are dependent on it and thus are vulnerable to both interruption of its use and usurpation of its capabilities*" (KUEHL, 2009).

RESUMO

O acesso a tecnologia e a utilização do ciberespaço, apesar de ainda não serem realidade universal - especialmente em países periféricos -, se encontram cada vez mais presentes no dia a dia da população mundial. Seja via aspectos de comunicação social, atividades financeiras, utilização de serviços públicos ou atividades militares, as diferentes camadas da sociedade, desde o nível individual ao nível estatal, utilizam o espaço cibernético e, portanto, estão vulneráveis aos riscos e ameaças presentes neste domínio. Nesse sentido, a pesquisa busca contribuir com os estudos de Segurança e Defesa, especialmente com a agenda de cibernética, e é impulsionada pelo seguinte problema: de que forma a estrutura de governança securitária do ciberespaço de um Estado pode afetar ações de Defesa Cibernética e de Segurança Cibernética? Para responder o problema de pesquisa são apresentados um pressuposto e duas preposições, presentes na introdução da pesquisa. O objetivo geral da pesquisa consiste em identificar de que forma a governança securitária do ciberespaço se relaciona com as ações de Defesa Cibernética e de Segurança Cibernética do Estado. A metodologia parte de uma abordagem qualitativa e o método hipotético-dedutivo é utilizado. São identificados cinco objetivos específicos, dispostos ao longo de três capítulos, com o intuito de conceituar termos como governança e governança securitária; explorar os termos Defesa Cibernética e Segurança Cibernética e suas aplicações; verificar se é possível separar Segurança e Defesa no ciberespaço e analisar como ocorre a operacionalização do ciberespaço por agentes estatais. São analisados trabalhos científico-acadêmicos, documentos oficiais de Estados e fontes jornalísticas. Além disso, também é utilizada a metodologia de estudos de caso comparados para verificar como Estados Unidos e Reino Unido têm abordado a questão da governança securitária do ciberespaço e estruturado (ou não) suas respectivas governanças securitárias do ciberespaço.

Palavras-chave: Ciberespaço. Governança Securitária do Ciberespaço. Defesa Cibernética. Segurança Cibernética. Estados Unidos. Reino Unido.

ABSTRACT

Both the access to technology and the use of cyberspace, despite not being a universal reality - especially in peripheral countries - are increasing its presence in the daily lives of the world's population. Whether it being through aspects of social communication, financial activities, use of public services or military activities, the different layers of society, from the individual level up to state level, use cyberspace and are therefore vulnerable to the risks and threats present in this domain. In this regard, the research seeks to contribute to Security and Defense studies, especially concerning the cyber agenda, and is driven by the following matter: in what aspects can the security governance's structure of a State's cyberspace affect Cyber Defense and Cyber Security? To answer the research question, an assumption and two prepositions are presented in the introduction. The general objective of the research is to identify how the security governance of cyberspace is related to the actions of Cyber Defense and Cyber Security of the State. The methodology starts from a qualitative approach and the hypothetical-deductive method is used. Five specific objectives are identified and arranged over three chapters in order to conceptualize terms such as governance and security governance; explore the terms and applications of Cyber Defense and Cyber Security; verify the feasibility of separating Security and Defense in cyberspace and analyze how cyberspace is operationalized by state agents. For this purpose, scientific-academic works, official documents from States and journalistic sources are analyzed. In addition, the comparative case studies methodology is also used to verify how the United States and the United Kingdom have approached the issue of cyberspace security governance and structured (or not) their respective cyberspace security governances.

Key words: Cyberspace. Cyberspace Security Governance. Cyber Defense. Cyber Security. United States. United Kingdom.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA - Advanced Research Projects Agency
CFTFs - Cyber Fraud Task Forces
CISA - Cybersecurity and Infrastructure Security Agency
DCA - Defesa Cibernética Ativa
DDoS - Distributed Denial of Service
DHS - Department of Homeland Security
DOD - Department of Defense
FBI - Federal Bureau of Investigation
FGV - Fundação Getúlio Vargas
GCHQ - Government Communications Headquarters
IC3 - Internet Crime Complaint Center
IFCs - Infraestruturas Críticas
IPTO - Information Processing Techniques Office
IPT - Information Processing Techniques Program
MI5 - The Security Service
MI6 - The *Secret Intelligence Service*
NASA - National Aeronautics and Space Administration
NCF - National Cyber Force
NCIJTF - National Cyber Investigative Joint Task Force
NCSC - National Cyber Security Centre
NSA - *National Security Agency*
ONGs - Organizações não Governamentais
ONU - Organização das Nações Unidas
OTAN - Organização do Tratado do Atlântico Norte
PNUD - Programa das Nações Unidas para o Desenvolvimento
SI - Sistema Internacional
TICs - Tecnologias da Informação e Comunicação
USCYBERCOM - United States Cyber Command
USSS - U.S. Secret Service

SUMÁRIO

1 INTRODUÇÃO

Com a virada do século XX para o século XXI, o ciberespaço apresentou um aumento significativo em sua quantidade de usuários, em um espectro que envolveu indivíduos, empresas, organizações e Estados. Para além da difusão e acesso à informação, da interdependência e das possibilidades de comércio interno e internacional, tais usuários perceberam que essa nova esfera também representaria ameaças e vulnerabilidades a serem identificadas e reconhecidas pelo Estado (CASHELL et al., 2004; TURK, 2005; DEVANNY et al., 2020). Ameaças essas que variam de ataques cibernéticos simples como phishing até ataques a infraestruturas críticas (IFCs)[1].

Como exemplo de ataque a IFCs, tem-se o Stuxnet, cujo alvo eram as usinas de enriquecimento de urânio em Natanz, no Irã. O *malware* atrasou o programa nuclear iraniano em anos (DE ARAÚJO, 2012) e demonstrou a capacidade de meios cibernéticos serem empregados para causar danos cinéticos à infraestruturas físicas. Diante dessas (e outras) ameaças, Estados têm percebido o ciberespaço como um ambiente propício à emergência de riscos à segurança nacional e, portanto, passível de ser introduzido a processos de securitização (LOBATO; KENKEL, 2015).

Tendo em vista o cenário atual, no qual Estados precisam estar aptos a lidar com as diversas possibilidades de ameaças e vulnerabilidades existentes no ciberespaço, o presente trabalho se propõe a analisar a governança securitária do domínio cibernético. Pretende-se investigar quais são os atores estatais (tanto da área de Segurança como de Defesa) responsáveis por identificar e lidar com os possíveis riscos e ameaças do ciberespaço, bem como identificar quais ações são atribuídas a órgãos de Segurança e quais ações são atribuídas a órgãos de Defesa. Para tornar tal objetivo tangível, o último capítulo do trabalho será utilizado para realizar uma análise comparada das governanças securitárias do ciberespaço de Estados Unidos e Reino Unido.

[1] Infraestruturas Críticas incluem a vasta rede de rodovias, conectando pontes e túneis, ferrovias, serviços públicos e edifícios necessários para manter a normalidade na vida diária. Transporte, comércio, água potável e eletricidade dependem desses sistemas vitais (ESTADOS UNIDOS, 2020).

A relevância da escolha de Estados Unidos e Reino Unido para a análise da governança securitária do ciberespaço no presente trabalho se justifica, primeiramente, pelo fato dos países ocuparem respectivamente a primeira e a terceira posição entre as trinta nações com maior poder no ciberespaço de acordo com o ranking realizado *pelo Belfer Center for Science and International Affairs* em 2020 (VOO et al., 2020). Ressalta-se, ainda, a relevância dos Estados selecionados serem considerados potências em suas respectivas regiões (NOLTE, 2010; FUCCILLE; REZENDE, 2013) e possuírem um papel fundamental na elaboração de documentos conjuntos sobre a temática de cibernética tanto no âmbito das Nações Unidas (ONU), como em organismos como a Organização do Tratado do Atlântico Norte (OTAN), entre outros.

Além disso, também foi levado em consideração o fato de Estados Unidos e Reino Unido representarem duas nações que executam ofensas cibernéticas de forma ativa, tendo o Brasil inclusive sido alvo de ofensas nos últimos anos, como revelado por Edward Snowden em 2013 (ABDENUR, 2014). É necessário salientar que isso não significa que Estados Unidos e Reino Unido apenas conduzam ações cibernéticas ofensivas e não sofram com elas, ou o contrário para o Brasil, mas sim que os dois países anglo-saxões possuem capacidades ofensivas mais avançadas do que o país sul-americano (UCHOA, 2013).

Sobre o domínio cibernético, Ventre (2012) destaca que este é composto por três camadas: a inferior, que é material e diz respeito à infraestrutura (*hardware*); a média, composta pelos sistemas de informação e de processamento de dados (*software*); e, por fim, a superior (cognitiva), referente ao caráter humano do ciberespaço. Libicki (2009), por sua vez, identifica a camada média como sintática, e enfatiza que esta é composta pela introdução das instruções que "designers e usuários dão à máquina e pelos protocolos por meio dos quais as máquinas interagem entre si" (LIBICKI, 2009, p. 12, tradução própria).[2]

[2] [Tradução própria]. No original, lê-se: *The syntactic level contains the instructions that designers and users give the machine and the protocols through which machines interact with one another*.

Ventre (2012) reflete sobre operações agressivas que podem ser realizadas no ciberespaço em cada uma das camadas que o compõem. Na inferior, o autor (2012) destaca os cortes de cabos submarinos de internet; na média, ressalta os ataques cibernéticos e os ataques de negação de serviço (DDoS); na superior, evidencia a desinformação, a influência, a manipulação e a batalha de ideias. Como argumentado por Guedes et al. (2017), a camada cognitiva é o ponto central da definição de Ventre, uma vez que é a partir do trabalho humano que se cria o espaço cibernético, diferentemente dos demais domínios. A partir dessas breves reflexões sobre o ciberespaço, fica perceptível o caráter da ligação entre diferentes componentes que permite a existência e funcionalidade desse domínio. Ao longo do primeiro capítulo da presente pesquisa, a discussão sobre ciberespaço será aprofundada.

No ciberespaço, os limites territoriais ainda não estão bem delimitados como nos outros domínios. Por conseguinte, o debate em torno de Segurança versus Defesa acaba por ser afetado, uma vez que este reflete a atuação do Estado interna e externamente. Os agentes estatais de Segurança, tradicionalmente, são responsáveis pela segurança interna do país, ao passo que os agentes de Defesa (no caso do Brasil, por exemplo: a Força Aérea, o Exército e a Marinha) são encarregados pela defesa externa, ou seja, responsáveis por lidar com ameaças oriundas de fora do território nacional.

A ausência de fronteiras delimitadas no ciberespaço dificulta uma ação imediata dos atores, principalmente se não houver diálogo constante entre eles sobre o tema. Devido a isso, Estados ainda estão elaborando suas estruturas de governança do ciberespaço da forma que julgam correta para que suas demandas específicas sejam atendidas conforme seus interesses e exposição dentro da esfera cibernética. Ressalta-se que a adoção de Defesa Cibernética ou Segurança Cibernética em documentos oficiais não se limita apenas a questões semânticas. A adoção de um termo ou outro impacta diretamente a forma pela qual se pensa a proteção e operacionalização do domínio cibernético e a governança para a elaboração de políticas públicas, como as políticas de defesa.

Com base na breve discussão apresentada acima sobre a governança securitária, o ciberespaço e o recorte de países escolhidos para a análise, tem-se o seguinte problema de pesquisa: de que forma a estrutura de governança

securitária do ciberespaço de um Estado pode afetar ações de Defesa Cibernética e de Segurança Cibernética? Apresenta-se um pressuposto e duas preposições:

Pressuposto 1: a estruturação da governança securitária de um Estado está diretamente relacionada às ações de Defesa Cibernética e de Segurança Cibernética deste Estado;

Preposição 1: a governança securitária do ciberespaço influencia o processo de securitização deste domínio;

Preposição 2: a escolha de utilização dos termos Segurança Cibernética ou Defesa Cibernética feita por um Estado, em documentos oficiais de Defesa, reflete na forma em que este Estado irá responder às ameaças no ciberespaço.

Tendo em vista o problema de pesquisa e o pressuposto, neste trabalho buscou-se entender se a governança securitária (ou formas de governança securitária) são capazes de afetar ações de Defesa Cibernética e Segurança Cibernética. Após análise, foi identificado que estruturas de governança securitária podem afetar ações de Defesa Cibernética e Segurança Cibernética. Entre os exemplos de estruturas que afetam as ações estão, por exemplo, forças-tarefa que unem diferentes órgãos para lidar com ameaças financeiras no ciberespaço ou para proteger infraestruturas críticas.

O objetivo geral da pesquisa consiste em identificar de que forma a governança securitária do ciberespaço se relaciona com as ações de Defesa Cibernética e de Segurança Cibernética do Estado. Os objetivos específicos são: i) conceituar governança e governança securitária; ii) explorar o que é Defesa Cibernética e o que é Segurança Cibernética; iii) estudar se, no ciberespaço, é plausível - ou não - fazer a separação entre Segurança e Defesa; iv) analisar como a operacionalização do ciberespaço por agentes estatais de Segurança e Defesa impacta na governança securitária deste domínio; e v) explorar a governança securitária estatal do ciberespaço em dois países: Estados Unidos e Reino Unido. Os dois países anglo-saxões foram escolhidos para a realização desta análise pelo fato de possuírem uma estrutura de governança estatal bem estabelecida no ciberespaço, pelo fator linguístico, pela documentação oficial disponibilizada e também por representarem dois dos Estados mais poderosos no ciberespaço.

Uma vez que se pretende analisar especificamente a operacionalização do ciberespaço por atores estatais, o recorte utilizado para o conceito de governança securitária irá considerar organismos vinculados ao executivo dos Estados, como agências de inteligência, sendo exemplos disso a *United States Intelligence Community* (que é composta por 17 agências governamentais independentes que atuam separadamente e em conjunto), a *Secret Intelligence Service* (MI6) do Reino Unido, agências de segurança, como a *National Security Agency* (NSA) no caso estadunidense, bem como agentes de Defesa, como as Forças Armadas de Estados Unidos e Reino Unido e as demais instituições estatais responsáveis pela Defesa Cibernética e Segurança Cibernética.

A seguir serão discutidos, brevemente, alguns pontos importantes para a presente dissertação que serão aprofundados no decorrer do trabalho. Sobre a securitização e fronteirização do ciberespaço, Demchak e Dombrowski (2011) apontam que esses fenômenos passam a ocorrer no momento em que o Estado percebe a necessidade de estabelecer regulamentações e legislações sobre o ciberespaço - bem como a necessidade de haver organismos responsáveis pela Defesa e Segurança Cibernética - para garantir a soberania nacional e a segurança da população. Tendo em vista que o ciberespaço evolui constantemente (PORTELA, 2018), os Estados precisam se adaptar para acompanhar essas transformações de maneira que consigam atuar nesse domínio da mesma forma que atuam nos demais: ar, espaço, mar e terra.

Já o conceito de governança securitária é definido por Caballero-Anthony (2019, p. 1) como "um conjunto de processos e arranjos realizados por uma série de atores estatais e não-estatais em vários níveis - do local ao internacional - que visam definir e gerenciar os desafios de segurança". Conforme Flemes e Radseck (2009), a governança securitária reflete a crescente fragmentação das estruturas de autoridade que lidam com questões de segurança internacional. Os autores destacam que a ordem de segurança atual possui, como característica, maior grau de fragmentação e complexidade do que o sistema de segurança centralizado da Guerra Fria. Nesse sentido, o conceito de governança securitária é construído não somente a partir da presença do Estado, mas também de empresas privadas, organizações não-governamentais, academia, entre outros (FLEMES; RADSECK, 2009).

Ainda sobre a governança securitária, Elke Krahmann (2003) discorre sobre a evolução de um sistema de segurança centralizado (durante a Guerra Fria) para um sistema cada vez mais fragmentado e complexo no que diz respeito às estruturas de segurança atuais. Flemes e Radseck (2009) compartilham a visão de Krahmann (2003) a respeito da fragmentação das estruturas de autoridade na governança securitária e adicionam à discussão três formas em que a governança securitária pode ocorrer: unilateral, bilateral ou multilateralmente. Para os fins deste trabalho, o conceito de governança será aplicado estritamente ao campo das políticas de Segurança e Defesa.

Segurança Cibernética e Defesa Cibernética são conceitos utilizados e elaborados por Estados, por meio de documentos oficiais de Defesa, bem como por acadêmicos. Ao analisar Defesa Cibernética e Segurança Cibernética, é necessário se ter em mente que não existem conceitos únicos definidos acerca do que um termo ou outro cobre; os termos podem ter significados distintos de acordo com o que aquele que os define deseja abordar (ROCHA, 2019). Posto isso, Galinec et al. (2017) discorrem sobre como a Defesa Cibernética foca na prevenção, na detecção rápida e no fornecimento de respostas que sejam efetivas a ataques ou ameaças, de maneira que seja possível evitar que qualquer infraestrutura crítica ou informação sigilosa venha a ser violada.

A discussão feita por Goldsmith (2013) vai um pouco além: o autor sugere, com base na crescente militarização do ciberespaço, que é possível identificar que, para além da proteção de sistemas críticos e computadorizados, a Defesa Cibernética pode acabar sendo, na verdade, uma capacidade ofensiva do Estado. De forma a abordar a Segurança Cibernética, Medeiros Filho (2014) associa o termo à dimensão da segurança pública. Para o autor, ao passo que a ciberdefesa está ligada a atos de guerra, a cibersegurança está relacionada a questões de ilegalidade, como o roubo ou sequestro de dados, por exemplo. Ressalta-se que o segundo capítulo deste trabalho irá explorar e discutir a temática de Defesa e Segurança Cibernética de maneira mais aprofundada.

Destaca-se que a ideia inicial do trabalho tinha como foco discutir o processo de securitização do ciberespaço pelo Estado a partir da metodologia da Escola de Copenhague. Porém, tendo em vista que esse objeto seria

bastante amplo para o período de mestrado (dois anos), optou-se pela realização do presente recorte, no qual será analisada a governança securitária estatal do ciberespaço. Espera-se, contudo, que a discussão a respeito da securitização do ciberespaço pelo Estado seja retomada no futuro doutorado.

Outra observação que deve ser feita é que, originalmente, a pesquisa contaria com três estudos de caso para analisar a governança securitária estatal do ciberespaço no terceiro capítulo: Brasil, Estados Unidos e Reino Unido. Todavia, ao longo do mestrado, percebeu-se que seria mais interessante focar nos estudos de caso de Estados Unidos e Reino Unido neste momento para que, ao decorrer da futura tese de doutorado, se analise a estrutura organizacional de Segurança e Defesa do Brasil voltada para o ciberespaço junto à outras potências médias, como Alemanha, Austrália, Coreia do Sul e Índia. O que se espera é criar uma lente de análise a partir das experiências de Estados Unidos e Reino Unido no ciberespaço, reconhecidamente atores poderosos, para melhor analisar a atuação de potências médias nesse domínio, bem como sugerir possíveis caminhos com base no que tem dado certo ou não nos casos explorados durante o mestrado.

O presente trabalho parte de uma abordagem qualitativa, que serve - entre outros fatores - para capturar e descobrir o significado de certo assunto (NEUMAN, 2004). Neste caso, analisar a governança securitária do ciberespaço e entender qual o impacto dessa governança na Defesa Cibernética e Segurança Cibernética de Estados. Ainda, optou-se pelo caráter qualitativo porque nele predomina a interpretação desenvolvida pelo pesquisador diante da compreensão do caso estudado, onde se observa "com aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e explicação da dinâmica das relações sociais" (SILVEIRA; CÓRDOVA, 2009, p. 32).

Para atingir os objetivos estabelecidos na pesquisa, será utilizado o método de estudos de caso comparados. Esse método tem como objetivo fornecer conhecimento concreto sobre um tema cujo caso é estrategicamente definido com base na representatividade das variáveis encontradas como relevantes em si ou em suas relações (neste caso, Governança Securitária como variável independente e Defesa Cibernética e Segurança Cibernética como variáveis dependentes). De acordo com Flyvbjerg (2006), os estudos de

casos se mostram úteis em etapas preliminares de investigações, devido ao fato de que eles fornecem hipóteses que podem ser "refutadas ou corroboradas sistematicamente com um número maior de casos" (FLYVBJERG, 2006, p. 220).

Para a realização da pesquisa sobre a operacionalização do ciberespaço por agentes estatais e o impacto disso na governança securitária do domínio, será empregado tanto o método de análise documental como o método de análise de eventos que tenham sido significativos no âmbito cibernético (como o caso Stuxnet; os episódios ocorridos na Estônia em 2007, entre outros), por meio de fontes acadêmicas e jornalísticas. Espera-se compreender, por meio da análise documental, quais agentes securitários para o ciberespaço são alocados pelo Estado. Todavia, também será utilizada a análise de eventos para explorar como a governança securitária de Estados Unidos e Reino Unido se posicionou em relação a eventos cibernéticos de grande impacto e verificar se a atuação do Estado, nesse contexto, foi condizente ou não com o que está disposto em documentos oficiais de Defesa.

Como citado anteriormente, para entender e analisar os dois contextos elencados para a pesquisa (Estados Unidos e Reino Unido), propõe-se a utilização da metodologia de estudos de caso comparados. De acordo com Goodrick (2014), estudos de caso comparados são realizados ao longo do tempo e servem para enfatizar a comparação dentro de e entre contextos. Nesse caso, entre os diferentes contextos de cada um dos países escolhidos para a análise. Ao se debruçar sobre a temática da governança securitária do ciberespaço de Estados Unidos e Reino Unido, espera-se poder - a partir da metodologia escolhida - analisar e sintetizar as similaridades, diferenças e possíveis padrões entre os três casos listados (GOODRICK, 2014). Entre as circunstâncias adequadas para a utilização desse método, Goodrick (2014) destaca perguntas de pesquisa que comecem com "como", "por que" e "de que forma", como a pergunta apresentada previamente nesta dissertação: de que forma a estrutura de governança securitária do ciberespaço de um Estado pode afetar ações de Defesa Cibernética e de Segurança Cibernética?

Para verificar como o espaço cibernético ressignifica os termos tradicionais já discutidos - como Segurança e Defesa -, é realizada revisão bibliográfica de artigos científicos sobre os assuntos em questão. Para efetuar

o levantamento de artigos sobre Defesa e Segurança Cibernética, bem como sobre a atuação de atores estatais e não-estatais no ciberespaço, foi explorado o portal da Biblioteca da Fundação Getúlio Vargas (FGV), que possui acervo de artigos revisados por pares mais amplo e abrangente do que o disponibilizado pelo Portal de Periódicos da CAPES[3]. A busca de artigos limitou-se às áreas de Ciência Política, Ciência e História Militar, Ciências Sociais e Humanas e, Relações Internacionais e Diplomacia. Para garantir a qualidade do que se busca nos artigos, foram utilizados como filtro os seguintes termos em inglês para obter número maior de resultados: cyber defense OR cyber defence; cyber security; cyberspace; state; defense OR defence.

Destaca-se o uso do método Snowball para encontrar novas fontes sobre os temas trabalhados no presente trabalho. Noy (2007) define o termo da seguinte forma: "um procedimento de amostragem pode ser definido como amostragem em bola de neve quando o pesquisador acessa os informantes por meio de informações de contato fornecidas por outros informantes" (NOY, p. 330, 2007, tradução própria). No caso, o autor se refere a acessar, de fato, pessoas. Todavia, para a realização desta pesquisa, o método será utilizado para encontrar novas fontes de conhecimento (artigos, livros, etc), utilizados por autores que já estão sendo explorados na pesquisa.

O trabalho é composto pela presente introdução, que representa o capítulo um, e por mais três capítulos, além das considerações finais. No segundo capítulo - por meio de revisão bibliográfica -, serão explorados e analisados conceitos como Governança, Governança Securitária, Ciberespaço, Poder e Poder Cibernético e o Sistema Internacional, de maneira a situar o leitor em qual contexto os conceitos Segurança e Defesa são empregados nas Relações Internacionais. Esse capítulo possui o intuito de montar o arcabouço teórico-conceitual necessário para a elaboração e compreensão dos demais capítulos.

No terceiro capítulo se explora os conceitos de Segurança e Defesa, além de se analisar os conceitos de Segurança Cibernética e Defesa Cibernética. Além disso, é estudado se, no espaço cibernético, é possível (ou não) fazer a separação entre Segurança e Defesa, o que é feito por meio de

[3] Como exemplo, ao contrário do portal da CAPES, o da FGV disponibiliza os periódicos científicos da EBSCO e Emerald.

revisão bibliográfica e de análise de documentos oficiais de Estados Unidos e Reino Unido. No quarto e último capítulo, será realizado estudo de caso comparado da governança securitária estatal do ciberespaço de dois países: Estados Unidos e Reino Unido. O propósito dessa comparação consiste em compreender quais são os atores estatais responsáveis por lidar com as ameaças no ciberespaço nos dois Estados e, também, verificar se a atuação deles no espaço cibernético condiz com as diretrizes expostas em seus documentos oficiais de Defesa. Por fim, serão expostas as considerações finais deste trabalho, onde serão discutidas as preposições da pesquisa, bem como o problema de pesquisa.

2 ELEMENTOS-CHAVE DA DINÂMICA DE GOVERNANÇA SECURITÁRIA NO CIBERESPAÇO: ANÁLISES TEÓRICAS

O presente capítulo tem como objetivo a exploração e análise dos conceitos necessários para a elaboração e compreensão da dissertação. Entre estes conceitos, estão Governança, Governança Securitária, Ciberespaço, Poder e Poder Cibernético. O intuito da análise desses conceitos consiste na elaboração de um arcabouço teórico-conceitual que sirva de auxílio para o desenvolvimento do trabalho como um todo, bem como para a compreensão e interpretação do trabalho pelos leitores.

Inicialmente será apresentada a discussão sobre Governança e Governança Securitária especificamente, que são elementos basilares para a construção da dissertação. Em seguida será realizada uma discussão sobre o ciberespaço, de forma a identificar diferentes conceitos e definições e analisar como esse novo domínio subverte de certa forma as relações internacionais e as tradicionais concepções sobre Segurança e Defesa. Também é realizado debate acerca de poder, poder cibernético e o Sistema Internacional pós Guerra Fria, de maneira a situar o leitor nas mudanças que ocorreram na agenda de segurança durante o período e que possuem encaminhamentos importantes para a atual agenda de Segurança e Defesa Cibernética.

2.1 GOVERNANÇA

Antes de adentrar a discussão sobre governança é necessário ter em mente que, assim como outros conceitos trabalhados na presente dissertação (ciberespaço, defesa cibernética, segurança cibernética, poder, entre outros), governança também é um conceito disputado e com diversas atribuições e significados, a depender de quem o está utilizando. Posto isso, de acordo com Peters (1998), a governança serve para aumentar a capacidade governamental de agir por meio de coalizões interorganizacionais estratégicas com atores para além do governo. Para tornar possível a compreensão acerca da governança (sua direção, prática e resultados), Peters (1998) indica que é necessário observar e interpretar o processo no qual a governança se desenvolve, bem como qual é o grau de influência dos atores envolvidos em tal sistema de

governança. Além disso, o autor ressalta que a governança, assim como outros modelos de serviço público, surge da cultura política em que está inserida. Portanto, é necessário ter em mente que, em diferentes contextos nacionais, surgirão distintas formas de governança.

Por seu turno, Fukuyama (2013) define governança como a capacidade de um governo estabelecer - e fazer serem cumpridas - leis, bem como a capacidade de prestar serviços à população. Nesse sentido, a governança é relacionada ao desempenho dos agentes na realização daquilo que é pedido pelos principais[4], e não aos objetivos estabelecidos pelos principais (FUKUYAMA, 2013). De forma resumida, a relação entre agente-principal é estabelecida da seguinte forma: o principal delega funções para o agente realizar em seu nome, desta forma, transferindo certo grau de autoridade para o agente (CAMPBELL, 2003; ULHØI, 2007). Ao pensar ações principal-agente no ciberespaço, um possível exemplo seria a contratação - por parte do Estado - de uma empresa fornecedora de serviços de segurança cibernética.

O quadro abaixo apresenta definições distintas para elucidar o conceito de governança.

Quadro 1 - Conceituações sobre governança

Autores	**Conceito de Governança**
Yong e Wenhao (2012)	Soma de muitas maneiras pelas quais indivíduos e instituições, públicas e privadas, gerenciam seus assuntos comuns.
Fukuyama (2013)	A capacidade de um governo estabelecer - e fazer serem cumpridas - leis, bem como a capacidade de prestar serviços à população.

[4] A teoria *principal-agent* representa a relação entre o proprietário (principal) de um ativo (empresas, bens de serviço, etc) e as pessoas (agentes) contratadas para gerenciar os ativos em nome do proprietário. No caso da governança discutida por Fukuyama (2013), o proprietário seria o governo, os ativos sendo gerenciados seriam as leis e a prestação de serviços à população e os agentes seriam os responsáveis pelos ativos em questão.

Mello e Slomski (2010)	Habilidade e capacidade do governo para: desenvolver com eficiência e responsabilidade a gestão dos recursos e das políticas públicas; tornar o governo mais aberto, responsável, transparente e democrático; promover mecanismos que possibilitem a participação da sociedade no planejamento, decisão e controle das ações que permitem atingir o bem comum.
Farrington (2009)	Engloba tanto a participação cidadã no governo como a entrega de bens e serviços-chave pelos governos.
Oliveira e Pisa (2015)	Envolve aspectos relacionados à gestão, transparência, prestação de contas, ética, integridade, legalidade e participação social nas decisões.

Fonte: elaborado pelo autor com base em Buta e Teixeira (2019).

A partir da tabela acima é possível inferir que o conceito de governança não possui apenas um significado: ele varia de acordo com as percepções daqueles que o definem. Por exemplo, ao passo que Yong e Wenhao (2012) conceituam a governança como as muitas maneiras pelas quais indivíduos e instituições gerenciam assuntos comuns, Fukuyama (2013) conceitua governança como a capacidade de um governo estabelecer - e fazer serem cumpridas - leis, bem como a capacidade de prestar serviços à população, representando assim dois significados bastante distintos para um mesmo termo.

Mello e Slomski (2010), por sua vez, apresentam a conceituação mais descritiva do termo entre as definições expostas. Para os autores, governança pode possuir diferentes significados. Como, por exemplo, a gestão de recursos e políticas públicas; a possibilidade de tornar o governo mais aberto de maneira eficiente, responsável, transparente e democrática e, por fim, pode ocorrer por meio da promoção de participação social no planejamento, decisão e controle de ações para o bem comum. Dessa forma, a definição estabelecida por Mello e Slomski (2010) também se distancia das definições de Yong e Wenhao (2012) e Fukuyama (2013). Todavia, as definições de Farrington (2009) e Oliveira e Pisa (2015) vão de encontro àquela feita por Mello e Slomski (2010). No caso de Farrington (2009), a "participação cidadã no governo" relaciona-se com a tentativa de tornar o governo mais aberto de forma transparente e responsável, como exposto por Mello e Slomski (2010). Já no caso de Oliveira e Pisa (2015), verifica-se a similaridade com Mello e Slomski (2010) no

momento em que os autores destacam a transparência e participação social na tomada de decisões.

Tendo em vista os conceitos apresentados, no presente trabalho o conceito de governança será entendido e utilizado como a coordenação da ação e tomada de decisão entre sociedade, atores estatais e atores não-estatais (como ONGs e empresas, por exemplo) sobre determinado assunto. Uma vez realizada a discussão sobre governança, na próxima seção se inicia o debate sobre uma forma mais específica de governança: a governança securitária. Como se percebe a partir da discussão realizada, o termo governança é bastante abrangente e pode possuir distintos significados. Portanto, nesta dissertação, optou-se por utilizar o termo governança securitária, de forma a discutir especificamente a governança entre atores estatais de Segurança e Defesa para o ciberespaço.

2.2 GOVERNANÇA SECURITÁRIA

Entre os principais conceitos aqui utilizados, está o de governança securitária. Usualmente, o termo é usado de forma a abordar as mais diversas agendas de segurança. No entanto, o recorte tem como foco o ciberespaço. Portanto, será utilizado o termo “governança securitária do ciberespaço” para que se torne possível compreender quais são os atores estatais atuantes no ciberespaço, sejam esses atores da área de Segurança ou Defesa. Ressalta-se, todavia, que o foco da análise é a atuação do Estado no ciberespaço devido ao recorte utilizado e ao período disponível para a realização da pesquisa. Portanto, atores não-estatais, como empresas de Segurança Cibernética, não farão parte da análise sobre a governança securitária deste domínio.

Como destacado na introdução da pesquisa, Caballero-Anthony (2019, p. 1) define governança securitária como "um conjunto de processos e arranjos realizados por uma série de atores estatais e não-estatais em vários níveis - do local ao internacional - que visam definir e gerenciar os desafios de segurança". Para Krahmann (2003, p. 11), governança securitária diz respeito às estruturas e processos que permitem a um conjunto de atores públicos e privados "coordenar suas necessidades e interesses interdependentes por meio da

tomada e implementação de decisões políticas vinculativas (em questões de segurança) na ausência de uma autoridade política central". Por sua vez, Kirchner (2006) define a governança securitária como um sistema internacional de regras que envolve a "coordenação, gestão e regulamentação de questões por autoridades distintas, intervenções de atores públicos e privados e arranjos formais e informais direcionados para resultados de políticas particulares" (KIRCHNER, 2006, p. 948).

Com base no que está exposto acima, torna-se claro que - apesar das definições apresentadas possuírem diferenças - existem elementos comuns abordados pelos autores nas características da governança securitária. Por exemplo: a multiplicidade de atores (públicos e privados); a coordenação de forma não hierárquica e, também, a combinação de mecanismos formais e informais (destacados na introdução de conceitos como processos e arranjos). Posto isso, é possível inferir que, diferentemente do conceito de governança, o qual é contestado por diversos autores possuindo inúmeros significados distintos, o conceito de governança securitária - apesar de mais recente - parece estar disposto de forma mais consensual entre os autores que o discutem.

Flemes e Radseck (2009) refletem sobre o contexto no qual a governança securitária é introduzida ao campo das Relações Internacionais: o final da Guerra Fria. Para os autores, a governança securitária demonstra a crescente fragmentação da estrutura de autoridade que lida com questões da agenda de segurança. Essa transformação, de acordo com os autores, ocorre devido a ausência de uma ameaça militar unificada. Nesse sentido, ocorre a ampliação das noções de segurança, de maneira a incluir um novo e maior leque de ameaças à segurança estatal e, portanto, surgem novos atores/mecanismos para a gestão da segurança internacional (FLEMES; RADSECK, 2009).

A governança securitária surge em um contexto de ascensão de estruturas e de processos que permitem a um conjunto de atores públicos e privados "coordenar suas necessidades e interesses via tomada e implementação de decisões políticas na ausência de uma autoridade política central" (KRAHMANN, p. 11, 2003; KRAHMANN, p. 20, 2005). Quando se pensa essa coordenação de ações no ciberespaço, é fato que existe esforço

por parte dos Estados no sentido de centralizar questões cibernéticas em aparatos estatais, como é o caso do *United States Cyber Command* (USCYBERCOM) nos Estados Unidos. No entanto, ao mesmo tempo em que é necessária uma resposta rápida para lidar com ameaças no ciberespaço, ainda é difícil determinar quando uma ameaça cibernética deve ser resolvida via agentes de segurança ou defesa (ou até mesmo via ações conjuntas). Com isso em mente, espera-se que a utilização do conceito governança securitária para analisar, entre outras coisas, a forma como vem sendo realizada a tomada de decisão dos Estados para resolver questões que envolvem o ciberespaço, possa ser útil ao campo de estudos de Defesa Cibernética e Segurança Cibernética.

Ao utilizar a discussão realizada por Arquilla e Ronfeldt (2001), Krahmann (2005) considera que o *networking* na área de políticas de segurança tem sido associado a difusão de poder que está ocorrendo para atores não-estatais, uma vez que estes possuem maior facilidade para se organizar em redes multi-organizacionais do que os atores tradicionais do Sistema Internacional, os Estados. Kirchner (2003) e Webber et al. (2004) identificam que ocorre algo como uma mudança de "governo", centralizado e focado no Estado, para uma governança que passa a ser multilateral e fragmentada.

Corroborando os argumentos de Kirchner (2003) e Webber et al. (2004), Krahmann (2005) aponta que a governança securitária tem adotado uma abordagem analítica descritiva para compreender a crescente fragmentação da formulação de políticas entre Estados, organizações internacionais e atores privados no Sistema Internacional. Similar aos pontos de Krahmann, Caballero-Anthony (2019, p. 1) discorre sobre como a governança securitária é definida como "um conjunto de processos e arranjos realizados por atores estatais e não-estatais em diferentes níveis (do local ao internacional)" de maneira que esses atores, em conjunto, definem e gerenciam os desafios presentes na agenda de segurança.

A estrutura de governança securitária apresentada por Kirchner e Dominguez (2014) é baseada em quatro dimensões, sendo elas as políticas de garantia, prevenção, proteção e *compellence*. De acordo com os autores, as políticas de garantia referem-se a medidas tomadas em situações de pós-

conflito. As políticas de prevenção, por sua vez, lidam com as causas que intensificam os conflitos e com a não-proliferação de armas de destruição em massa. As políticas de proteção têm como objetivo principal proteger a sociedade de ameaças externas, como terrorismo, crime organizado e corrupção. Já as políticas de *compellence* envolvem intervenções humanitárias ou, até mesmo, operações de imposição da paz (KIRCHNER; DOMINGUEZ, 2014).

A partir das quatro dimensões da estrutura de governança securitária de Kirchner e Dominguez, é possível enquadrar tanto ações de Segurança Cibernética como de Defesa Cibernética. As políticas de garantia, que os autores colocam como políticas utilizadas no pós-conflito, por exemplo, remetem às ações de Defesa Cibernética, como a obtenção de informações e a restauração de sistemas danificados. As políticas de prevenção, como o nome já prevê, podem ser correlacionadas às ações de prevenção contra ameaças ou possibilidade de ameaças. As políticas de proteção contra ameaças externas também se relacionam com a Defesa Cibernética, como as ações ofensivas e defensivas, que serão destacadas com base em Estados Unidos e Reino Unido, para combater oponentes. Já as políticas de *compellence*, que usualmente representam a capacidade de coerção de um Estado por meio de ameaça, podem ser entendidas como similares à definição de Defesa Cibernética Ativa do Reino Unido e Dewar (2014), no que diz respeito às medidas proativas de combate e defesa contra ameaças.

De forma a analisar o caráter geográfico da governança securitária, Villa (2017), prevê que diferentes regiões geográficas exibem lógicas distintas de governança securitária. Se espera que, quando analisados os casos de governança securitária estatal do ciberespaço de Estados Unidos e Reino Unido, torne-se possível verificar (ou não) a veracidade desta afirmação neste contexto. Apesar da ótica deste trabalho estar voltada para a atuação do Estado especificamente, é importante destacar que, conforme Villa (2017), tradicionalmente, grupos domésticos não se concentram em questões de política externa ou segurança, mas isso tem mudado.

Normalmente, a atuação de Estados no sentido de políticas de Defesa e Segurança é mais restrita a uma pequena elite (VILLA, 2017). Todavia, Villa destaca que, nas últimas décadas, o monopólio do Estado em questões de

segurança vem sendo questionado, tanto internamente como por atores extrarregionais. Entre os motivos pelos quais esse cenário tem mudado, de acordo com o autor, estão, por exemplo, a ascensão de questões indígenas, de minorias, de meio ambiente, entre outras, na agenda de segurança. Dessa forma, atores não-estatais como empresas militares privadas e organizações não-governamentais estão cada vez mais atuando na agenda de segurança junto a atores estatais. Contudo, devido ao período de tempo para a realização da presente pesquisa (dois anos), optou-se apenas pela análise de atores estatais na governança securitária do ciberespaço no presente momento, com a possibilidade de maximizar a pesquisa de forma a abranger esses atores no futuro doutorado.

2.3 CIBERESPAÇO

Parker (1993), ao analisar o ciberespaço, o definiu como o conjunto completo das redes de comunicações (públicas e privadas), de maneira a incluir telefones de redes públicas; redes de dados em pacotes e redes puras de computadores - incluindo a internet e sistemas de comunicação sem fio, como celulares. As principais vulnerabilidades no ciberespaço identificadas pelo autor incluem "fraquezas processuais, administrativas e humanas nas redes de comunicação, e não vulnerabilidades puramente técnicas de gerenciamento de rede ou sistemas de controle, hardware ou software" (PARKER, 1993, p. 16). Segundo o autor, as vulnerabilidades técnicas são, usualmente, exploradas a partir de fraquezas processuais, administrativas ou humanas.

Por sua vez, Libicki (2009) define o ciberespaço como um meio virtual menos tangível do que a terra, o mar, o ar e até mesmo o espaço. De acordo com o autor, para entender o ciberespaço é preciso identificar as três camadas que o compõem: a camada física, a camada sintática (acima da camada física) e a camada semântica (que fica no topo). A camada física é composta por caixas e fios e armazena todos os sistemas de informação. A camada sintática, por sua vez, contém as instruções que os usuários enviam às máquinas e os protocolos pelos quais as máquinas interagem entre si. Por fim, a camada semântica é a que detém as informações contidas na máquina (LIBICKI, 2009).

A definição de Ventre (2012), brevemente explorada na introdução desta pesquisa, também divide o ciberespaço em três camadas: a camada inferior, que é material e diz respeito à infraestrutura (*hardware*); a camada média, que é a camada dos sistemas de informação e do processamento de dados (*software*); e, por fim, a camada superior (cognitiva), que diz respeito ao caráter humano do ciberespaço. Apesar de os dois autores argumentarem que o ciberespaço é composto por três camadas, é notável que existem distinções entre as camadas identificadas por eles. Ao passo que Ventre considera a camada superior como o componente humano do ciberespaço, Libicki enxerga esta camada como a que detém as informações contidas na máquina.

Ao discorrer sobre o ciberespaço, Rattray (2009) postula que este é, também, um ambiente físico. O autor salienta que, pelo fato de possuir sistemas físicos (para além dos sistemas de redes, *software* e protocolos de comunicação), o ciberespaço pode ser considerado como um ambiente misto, presente tanto na realidade física como na realidade virtual. A dualidade do ciberespaço identificada por Rattray (2009), a qual coloca o domínio cibernético tanto como pertencente ao mundo físico como virtual, é também salientada por Ventre (2012) no momento em que o autor discute as camadas de *hardware* e *software*. Para Ventre, o *hardware* significa tudo aquilo que faz parte do espaço cibernético e é material, tangível. Como por exemplo, os cabos submarinos e os satélites. Já o *software*, conforme Ventre, diz respeito àquilo que não é material no ciberespaço, como os sistemas de informação e o processamento de dados, presentes na parcela virtual do ciberespaço apresentada por Rattray (2009).

Assim como Rattray, Sheldon (2011) também explora o caráter físico do ciberespaço. Todavia, o autor vai um pouco além de Ventre e Libicki. Para ele, o ciberespaço é composto não apenas por três, mas sim por quatro camadas: infraestrutura, física, sintática e semântica. Sobre as camadas, Sheldon afirma que

> A camada de infraestrutura consiste em *hardware*, cabeamento, satélites, instalações e assim por diante. A camada física consiste na miríade de propriedades de elétrons, fótons, frequências e assim por diante - que animam a camada de infraestrutura. A camada sintática consiste na formatação das informações e nas regras que instruem e controlam os sistemas de informação que compõem o ciberespaço. A camada semântica consiste em informações úteis e compreensíveis

> para usuários humanos e é essencialmente o nexo cibercognitivo[5] (SHELDON, 2011, p. 98).

Nota-se uma diferença significativa entre a concepção de Sheldon e as de Ventre e Libicki: Sheldon separa a camada de infraestrutura da camada física. Sheldon corrobora com as visões de Ventre e Libicki no que diz respeito à camada de infraestrutura (apesar dos outros dois autores chamarem essa camada de física, e não de infraestrutura), sendo esta referente ao *hardware*, ou seja, cabos, satélites e instalações físicas em geral. A grande diferença se encontra na adição do que Sheldon chama de camada física, composta por propriedades de elétrons, fótons e frequências que servem para animar a camada de infraestrutura (a mesma camada física/*hardware* de Ventre e Libicki).

Em paralelo, Kuehl (2009) oferece uma definição própria sobre o ciberespaço:

> o ciberespaço é um domínio global dentro do ambiente de informação, cujo caráter distinto e único é enquadrado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação (KUEHL, 2009, p. 4).

O que se sobressai na definição do autor é que, diferentemente das definições apresentadas por Libicki (2009), Sheldon (2011) e Ventre (2012), esta não foca nas camadas presentes no ciberespaço (não obstante, identificam-se paralelos entre o espectro eletromagnético e a camada física de Sheldon). O autor caracteriza o ciberespaço como um domínio global que existe dentro do ambiente informacional e, então, discorre sobre o que pode ser feito neste domínio, como a criação, armazenamento, modificação, troca e exploração de informações.

Abaixo será exposto quadro referente às definições de ciberespaço presentes nos documentos oficiais de Defesa elaborados por Estados Unidos e Reino Unido - países em análise nesta pesquisa - com o intuito de verificar a similaridade (ou não) do que é compreendido sobre o termo para eles.

---

[5] [Tradução própria]. No original, lê-se: *The infrastructure layer consists of the hardware, cabling, satellites, facilities, and so on. The physical layer consists of the myriad properties of the EMS—electrons, photons, frequencies, and so forth— that animate the infrastructure layer. The syntactic layer consists of the formatting of information and the rules that instruct and control information systems that make up cyberspace. The semantic layer consists of information useful and comprehensible to human users and is essentially the cyber-cognitive nexus*.

Também será analisada a definição apresentada no Manual de Tallinn (2017) da Organização do Tratado do Atlântico Norte (OTAN), uma vez que Estados Unidos e Reino Unido são membros da Organização. Como será possível identificar, existem similaridades entre as definições dos Estados e as definições trabalhadas anteriormente com base em autores como Kuehl, Libicki, Sheldon, Ventre e Rattray.

Quadro 2 - Definições de ciberespaço para Estados Unidos, Reino Unido e OTAN

País	Definição
Estados Unidos	Um domínio global dentro do ambiente de informação que consiste em redes interdependentes de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores incorporados.[6]
Reino Unido	A rede interdependente de infraestruturas de tecnologia da informação, que inclui a Internet, as redes de telecomunicações, os sistemas informáticos, dispositivos ligados à Internet e os processadores e controladores incorporados. Pode se referir também ao mundo ou domínio virtual enquanto experiência ou conceito abstrato.[7]
OTAN	O ambiente formado por componentes físicos e não físicos para armazenar, modificar e trocar dados usando redes de computadores.[8]

Fonte: elaborado pelo autor com base em Estados Unidos (2021), Reino Unido (2016) e OTAN (2017).

Conforme a tabela acima, pode-se compreender o que Estados Unidos, Reino Unido e OTAN definem como ciberespaço. As definições dos Estados Unidos e Reino Unido são bastante similares: ambas destacam o meio digital, as infraestruturas físicas e, também, o componente humano do ciberespaço. O

[6] [Tradução própria]. No original, lê-se: *A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*

[7] Definição da Estratégia Nacional de Segurança Cibernética 2016-2021 do Reino Unido, disponível em português.

[8] [Tradução própria]. No original, lê-se: *The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks*.

caráter físico do ciberespaço, para esses dois Estados, também está presente quando são discutidos os "processadores", que são as máquinas e infraestruturas nas quais as informações são armazenadas.

Os conceitos apresentados por Estados Unidos e Reino Unido remetem à discussão sobre o ciberespaço apresentada por Kuehl (2009). Os Estados Unidos, por exemplo, conceituam o ciberespaço, antes de mais nada, como um domínio global, assim como o autor. Além disso, tanto Estados Unidos como Reino Unido fazem menção às redes interdependentes por onde as informações percorrem, o que também está presente na concepção de Kuehl. Todavia, Estados Unidos e Reino Unido elucidam as infraestruturas, que representam o componente físico do ciberespaço, como discutido por Libicki (2009), Rattray (2009), Sheldon (2011) e Ventre (2012). Ademais, a conceituação de Parker (1993), que define o ciberespaço como o conjunto de redes de comunicações, também é similar às definições dos Estados Unidos e Reino Unido, que salientam as redes de telecomunicações.

Em suas definições de ciberespaço, Estados Unidos e Reino Unido incorporam o conceito de "controladores". Entretanto, os países não especificam o que seriam esses sujeitos. O dicionário Oxford define controlador tanto como "uma pessoa que administra ou dirige algo" ou como "um dispositivo que controla ou regula uma máquina ou parte de uma máquina", o que abre margem para que os controladores expostos na definição desses dois Estados possam, de fato, ser referentes ao componente humano do ciberespaço.

Skinner (2013) utiliza a mesma definição de ciberespaço do Departamento de Defesa dos Estados Unidos (DoD) e, segundo o autor, os "controladores" são parte do efetivo alocado para lidar com a defesa do domínio cibernético. Skinner cita, entre os especialistas presentes no ciberespaço, os controladores de operações, controladores de eventos, controladores de operações cibernéticas defensivas e ofensivas e controladores de operações de rede de informação. Similar a Ventre (2012), que discute o caráter cognitivo/humano do ciberespaço, os dois países em questão colocam os "controladores incorporados" ao ciberespaço em seus textos, que basicamente são os humanos responsáveis pela tomada de decisão do Estado no domínio cibernético. Ressalta-se que essas definições

foram extraídas de documentos oficiais de Defesa, e, ao analisá-las, percebe-se que possuem caráter mais direto e abrangente, uma vez que, se o ciberespaço for definido de forma mais específica e crítica, o Estado pode acabar limitando sua própria atuação no domínio.

Conforme Walden (2010), o ciberespaço pode ser visto como a rede de comunicação transnacional definitiva, tendo em vista que oferece uma capacidade incomparável de acesso a dados e sistemas a nível global. No entanto, o autor argumenta que, apesar dos benefícios, essa esfera também pode servir como fonte de vulnerabilidades para o Estado, seja via conflitos políticos, liberalismo econômico ou ciberterrorismo. Assim como os Estados Unidos e o Reino Unido, que incluem a importância das infraestruturas de tecnologia e informação em suas definições de ciberespaço, Walden (2010) argumenta que, ao passo que as economias ao redor do globo e as sociedades se tornam dependentes do espaço cibernético, este se torna uma "infraestrutura de informações críticas sobre a qual quase todos os governos, talvez com exceção dos Estados Unidos, têm controle limitado" (WALDEN, 2010, p. 66).

Ao discorrer sobre o ciberespaço, a Organização do Tratado do Atlântico Norte (OTAN) oferece duas definições para o termo ao longo do tempo, ambas divulgadas por intermédio do Manual de Tallinn (versões de 2013 e 2017). Na primeira versão, a OTAN caracteriza o ciberespaço como "o ambiente formado por componentes físicos e não físicos, caracterizado pelo uso de computadores e pelo espectro eletromagnético para armazenar, modificar e trocar dados por meio de redes de computadores" (OTAN, 2013, p. 211, tradução própria).

Todavia, na atualização do Manual em 2017, presente no quadro anteriormente apresentado, a organização modifica a definição do conceito, agora visto como: "o ambiente formado por componentes físicos e não-físicos para armazenar, modificar e trocar dados por meio de redes de computadores" (OTAN, 2017, p. 563). A definição da Organização se aproxima das definições de Libicki, Rattray, Sheldon e Ventre no que diz respeito à existência de componentes físicos e não-físicos na composição do ciberespaço. Além disso, a OTAN também ressalta, pelo menos na versão do documento de 2013, o caráter eletromagnético do ciberespaço - assim como Kuehl - bem como a possibilidade de armazenamento, modificação e troca de dados.

Tendo em vista que Estados Unidos e Reino Unido são membros da Organização, julga-se relevante comparar as definições estabelecidas pelos dois Estados com o que é disposto pela OTAN. Um ponto que chama atenção na definição de ciberespaço para a OTAN é que, pela forma como a Organização descreve o termo, o torna ainda mais vago e enxuto do que as versões de Estados Unidos e Reino Unido. Ao definir o ciberespaço de forma vaga, a OTAN, de certa forma, pode estar ampliando o seu escopo de atuação no domínio, uma vez que não são estabelecidos limites do que faz ou não parte do ciberespaço. Apenas é exposto que esse domínio é formado por componentes físicos e não-físicos, sem qualquer especificação, diferentemente do que ocorre nas definições de Estados Unidos e Reino Unido, que expõem os componentes do ciberespaço. Além disso, mesmo que Estados Unidos e Reino Unido possuam definições próprias mais robustas do termo, os países podem tirar proveito das entrelinhas existentes na definição da OTAN na hora de atuar no ciberespaço e de o definir, visto que o termo é bastante vago, especialmente se estiverem atuando em nome da Organização.

As duas definições trazidas pela OTAN de fato são bastante similares. Entretanto, na atualização do documento, em 2017, foi retirado o espectro eletromagnético da definição, que é parte essencial do ciberespaço. Conforme discussão realizada por Medeiros (2019), os efeitos da operacionalização do espectro eletromagnético se manifestam na camada física do domínio cibernético, camada esta que se encontra nos domínios tradicionais como terra ou mar e, consequentemente, em territórios nacionais, o que pode gerar distintas reações (MEDEIROS, 2019).

Com base em tudo o que foi discutido sobre o conceito até aqui, a definição a ser utilizada neste trabalho compreende o ciberespaço como um domínio composto por três camadas: física, sintática e humana. A camada física representa o componente tangível do ciberespaço, como os cabos submarinos, satélites e todo *hardware* em geral; a camada sintática diz respeito ao *software*, às instruções enviadas às máquinas e a comunicação própria que ocorre entre as redes computadorizadas e, por fim, a camada humana representa o tomador de decisão no ciberespaço, bem como o componente cognitivo que constrói esse domínio diariamente.

Hansen e Nissenbaum (2009) escrevem sobre a crescente preocupação com a segurança no ciberespaço. Para os autores, a magnitude e simultaneidade dos ataques realizados no domínio cibernético pode ter efeitos em cascata, o que significa que os danos podem ir para além das redes e atingir infraestruturas físicas, por exemplo. Além disso, é demonstrada preocupação com o fato de os computadores terem, de certa forma, dissolvido as fronteiras tradicionais que protegiam o Estado-nação. Para fortalecer esse argumento, Hansen e Nissenbaum utilizam *The National Strategy* (2003) e Yould (2003), ao dizer que "a infraestrutura que compõe o ciberespaço - *software* e *hardware* - é global tanto em seu design como em seu desenvolvimento" e que os ciberatacantes podem operar à distância, de forma a ofuscar sua "identidade, localização e locais de entrada"[9] (HANSEN; NISSENBAUM, 2009, p. 1161).

Sobre as operações que ocorrem no ciberespaço, Poduval (2012) destaca o caráter que elas possuem de não poderem ser ouvidas, vistas ou sentidas no sentido literal (diferentemente de uma invasão tradicional no mundo físico, onde é possível ver o processo acontecer). Conforme o autor, no domínio cibernético, um *malware* pode residir no sistema sem o hospedeiro perceber, ao mesmo tempo em que o *malware* envia os dados de interesse para quem o controla em algum lugar do globo (PODUVAL, 2012). Entre os muitos problemas de segurança existentes no ciberespaço, Poduval enfatiza a não existência de sinais visíveis de entrada ou saída no domínio como os principais.

Questões como a preocupação com a segurança no espaço cibernético trabalhada por Hansen e Nissenbaum (2009), bem como a dificuldade em identificar o local exato no qual são realizadas as operações no ciberespaço, como discutido por Poduval (2012), levantam o debate sobre a possibilidade de fronteirização ou até mesmo a adequação de uma geografia do ciberespaço. O que poderia, de certa forma, ajudar a estabelecer limites que permitam a identificação do que é feito pelos usuários neste domínio e de estabelecer até onde essa atuação pode ir. No entanto, surge a seguinte pergunta: até que

[9] [Tradução própria]. No original, lê-se: ‘‘*the infrastructure that makes up cyberspace—software and hardware—is global in its design and development’’ and cyber attackers may operate at a distance obfuscating ‘‘their identities, locations, and paths of entry*’’.

ponto é possível estabelecer limites ou barreiras geográficas em um domínio tão fluido e em constante evolução como o ciberespaço?

Milton Santos (2002) reconhece as mudanças decorrentes da tecnologia para a geografia. Segundo o autor:

> os espaços assim requalificados atendem sobretudo aos interesses dos atores hegemônicos da economia, da cultura e da política e são incorporados plenamente às novas correntes mundiais. O meio técnico-científico-informacional é a cara geográfica da globalização (SANTOS, 2002, p. 239).

Dessa forma, Santos (2002) afirma a possibilidade de territórios tradicionais serem transformados a partir da tecnologia e globalização. Por sua vez, Medeiros (2019) discute as lógicas reticular e zonal. A lógica reticular, para o autor, representa a conexão entre diferentes dispositivos físicos e os fluxos de informação que percorrem as chamadas infovias. A lógica zonal, por sua vez, representa a conceituação tradicional de território, ou seja, aquele que é delimitado por fronteiras.

O que Medeiros (2019) salienta sobre a geografia do ciberespaço é que, devido ao enorme grau em que a sociedade moderna está inserida no meio tecnológico, a lógica reticular do espaço cibernético passou a atravessar a lógica zonal dos territórios. Isso significa, basicamente, que as fronteiras territoriais (lógica zonal) passaram a ser passíveis de penetração via ciberespaço, sem a necessidade de qualquer invasão física, uma vez que é possível transpassar a barreira física via lógica reticular estando em qualquer lugar do globo. Interessante verificar que a possibilidade de penetrar fronteiras territoriais via ciberespaço sem a necessidade de qualquer invasão tradicionalmente geográfica vai justamente de encontro às preocupações elencadas por Hansen, Nissenbaum e Poduval.

O argumento de Nielsen (2012) é que o ciberespaço caracteriza um ambiente que relativamente não possui fronteiras. Relativamente porque, segundo Nielsen, a geografia do ciberespaço não é totalmente imaterial. Essa constatação vai de encontro ao argumento de Medeiros e Goldoni (2020), o qual salienta que o domínio cibernético está parcialmente dissociado do espaço físico. Para além disso, Nielsen argumenta que a geografia do ciberespaço é menos significativa do que nos outros domínios (como ar, mar ou terra), devido

ao fato de ser mais complicado determinar o que é território doméstico e o que é estrangeiro nesse domínio (NIELSEN, 2012).

Essa discussão representa caráter importante para a presente pesquisa porque, uma vez que a lógica zonal é transposta pela lógica reticular, dificulta-se a alocação de atores estatais no ciberespaço. Isso acontece devido à dificuldade de compreensão do que faz parte do território interno e o que faz parte do âmbito externo, que é a base de definição para atuação de agentes de Segurança ou Defesa. Dessa forma, o ciberespaço desafia tanto os conceitos tradicionais como a alocação tradicional de atores estatais no que diz respeito ao combate a ameaças.

2.4 SISTEMA INTERNACIONAL, PODER E PODER CIBERNÉTICO

O efeito da queda da União Soviética no Sistema Internacional, ao final da Guerra Fria, foi o maior desde a Segunda Guerra Mundial no sentido de mexer com a configuração de Estados no âmbito internacional. Conforme Wohlforth (1999), a estrutura bipolar estabelecida entre Estados Unidos e União Soviética durante quase meio século foi o que determinou a agenda e as políticas de Segurança naquele período. O autor indica que, com o surgimento da unipolaridade estadunidense a partir da década de 1990, a competição securitária entre grandes potências passou a diminuir.

Portanto, a partir do final da década de 1980 com o término da Guerra Fria, a agenda de segurança passou a ser ampliada e a abordar assuntos para além de ameaças militares estatais. Nesse sentido, passou a ser reconhecido que estava ocorrendo mudanças na natureza das ameaças e que, inevitavelmente, os conflitos não se encaixariam mais nos moldes tradicionais de guerra entre Estados. A agenda de segurança passou, então, a se tornar além de mais ampla, mais liberal, o que ocorreu devido ao fato de o projeto estadunidense ter obtido sucesso, projeto esse que necessitava a existe de um Sistema Internacional aberto e interligado para funcionar.

De acordo com Wohlforth (1999), a diminuição de competição entre grandes potências veio a acontecer porque, uma vez que os Estados Unidos se estabeleceram como líder do sistema, o país passou a possuir os meios (e os

motivos) para manter instituições-chave na área de Segurança. De acordo com o autor, esse protagonismo estadunidense ocorreu de forma a reduzir tanto os conflitos de segurança locais, como os custos de competição entre grandes potências. Inclusive, é possível que a própria perpetuação de uma “agenda cibernética” na área de Segurança se deva aos Estados Unidos como ator unipolar no Sistema Internacional (pelo menos nos anos 1990).

Por outro lado, Waltz (1979) defende que o Sistema Internacional (SI) não pode e não deve ser explicado de maneira reducionista. De acordo com o autor, uma teoria mais robusta de Relações Internacionais deve surgir a partir de uma abordagem sistêmica, na qual o Sistema Internacional representa uma estrutura formada por unidades (Estados). Por sua vez, a ação (ou reação) dos Estados no Sistema Internacional pode ser explicada a partir das pressões exercidas sobre aqueles pela constante competição entre os países no cenário internacional. A competição ocorre nos mais diversos níveis: securitário, econômico, social e político (nesta pesquisa, o foco será as agendas de Defesa e Segurança dos Estados). Ressalta-se que países possuem objetivos diversos no Sistema Internacional, todavia, existe algo que todos buscam nesta estrutura descentralizada e anárquica: a sobrevivência (WALTZ, 1979).

Waltz (1979) também compara o que acontece no âmbito interno dos países com o próprio Sistema Internacional. No âmbito interno, existem instituições e uma hierarquia entre elas, além do governo como regulador central. Entretanto, no Sistema Internacional, a situação é bastante diferente. E isso ocorre devido ao fato de que no Sistema Internacional não existe uma hierarquia estabelecida, justamente pelo fato de não haver um Leviatã supranacional, por isso é instituída a chamada anarquia. Assim como Waltz, Mearsheimer (2001) entende que o comportamento dos Estados no Sistema Internacional é moldado pela anarquia. No entanto, o autor afirma que isso não caracteriza desordem: apenas a inexistência de uma unidade governamental que governe a todos Estados inseridos no Sistema Internacional.

De acordo com Brooks (1997), realistas pós-clássicos não assumem a ideia de que os Estados sempre considerarão o pior cenário possível, e sim que tomarão decisões baseadas na probabilidade de haver problemas relacionados a sua segurança. Além disso, Brooks argumenta que os realistas pós-clássicos partem da ideia de que os Estados perseguem poder e não

segurança em si. Mearsheimer (2001) diferencia-se dos realistas pós-clássicos como Brooks (1997) pois, para o realismo ofensivo, a segurança, ou seja, a sobrevivência do Estado, sempre será a prioridade estatal.

É exatamente a necessidade de garantir a sobrevivência estatal que vai fazer com que Estados atuem de maneira ofensiva no Sistema Internacional, de acordo com Mearsheimer. O autor também reflete sobre a questão da agressão calculada, a qual discute a forma como todos os Estados gostariam de obter uma posição de destaque no Sistema Internacional, mas que é impossível pois nem todos possuem as capacidades necessárias para tal. Consoante o autor: "todo Estado pode querer ser o rei da colina, mas nem todo Estado tem os recursos para competir por essa posição elevada, muito menos alcançá-la" (MEARSHEIMER, 2001, p. 02, tradução própria).[10]

Nesse sentido, um questionamento interessante a se levantar seria se o ciberespaço não poderia significar, no Sistema Internacional, um agente democratizador para a difusão de poder. Visto que atores não-estatais e Estados de menor relevância (em termos de capacidades militares, por exemplo), conseguem atuar ativamente por meio desse domínio com custos menores do que os que seriam necessários para atuar em domínios tradicionais como terra e mar. Para Nye (2011), as características do ciberespaço (como o fácil acesso e alcance) diminuem alguns diferenciais de poder entre os atores e, a partir disso, podem ser utilizadas como um exemplo de difusão de poder.

O autor ainda argumenta que, dificilmente, grandes potências conseguirão dominar o ciberespaço da mesma forma que dominam o mar ou o ar, tendo em vista que neste domínio há grande multiplicidade de atores constantemente atuantes para além dos Estados. Todavia, Nye (2011) admite que apesar de haver certa difusão de poder no ciberespaço, de forma alguma isso significa que haja igualdade ou simetria de poder entre os atores presentes neste domínio. Qualquer simetria de poder entre Estados é difícil porque Estados já poderosos militar e economicamente, como Estados Unidos e Reino Unido, têm capacidade maior de investir de forma acentuada no

[10] [Tradução própria]. No original, lê-se: *every state might want to be king of the hill, but not every state has the wherewithal to compete for that lofty position, much less achieve it*.

desenvolvimento de tecnologias e capacidades cibernéticas, o que os distancia de atores menores.

Mearsheimer (2001) admite que uma grande potência - quando em confronto com outro oponente poderoso - estará menos inclinada a ser ofensiva e mais preocupada com a defesa do equilíbrio já existente (*status quo*), de forma a tentar garantir sua sobrevivência. Antes de Estados tomarem decisões de ofensa, eles irão racionalmente calcular quais são suas possibilidades de ganhos e perdas e, então, decidir se devem ou não atacar seu possível inimigo (MEARSHEIMER, 2001). Percebe-se, a partir de Mearsheimer (2001), a condição da segurança do Estado mais vinculada à sobrevivência do mesmo, ao passo que a defesa volta seus esforços para manter o *status quo* existente, evitando perdas.

Para Morgenthau (2003) "a política do *status quo* visa à manutenção da distribuição do poder que existe em um momento particular na história" (MORGENTHAU, 2003, p. 89). Em outras palavras, *status quo* significa a manutenção da forma como a distribuição de poder entre Estados ocorre no Sistema Internacional ao longo da história, sendo o *status quo* o mantenimento da ordem atual, ou seja, a continuação da ordem de poder que está estabelecida. Entretanto, quando houver um Estado detentor de demasiado poder sozinho, outros Estados podem escolher formar uma aliança para contestar o *status quo* atual e modificá-lo, o que poderia alterar a balança de poder.

Especificamente sobre a balança de poder, Morgenthau argumenta que, no que diz respeito à política internacional, forças automáticas começam a atuar no momento em que algum Estado se dedica a expandir seu poder. O que essas "forças" fazem é, basicamente, um esforço na direção de manter o equilíbrio de poder no Sistema Internacional, de forma a não permitir que um Estado sozinho acumule poder demais. Para o autor, o equilíbrio da balança de poder é instrumento necessário para garantir que a paz seja mantida no Sistema Internacional (MORGENTHAU, 2003, p. 45). Wohlforth (2012) retoma a discussão acerca da unipolaridade no Sistema Internacional. De acordo com o autor, *balance-of-power realists* - como Christopher Layne -, argumentam que a unipolaridade rapidamente gera uma pressão sistêmica que move o Sistema Internacional de volta para a multipolaridade. Wohlforth considera que nessa

afirmação não apenas falta reflexão, como ela também constitui uma aplicação inadequada da teoria da balança de poder.

Nesse sentido, Layne (1993, p. 5) define unipolaridade como "um sistema contendo um poder cujas capacidades são formidáveis o suficiente para impedir a formação de uma coalizão de equilíbrio esmagadora contra ele". Assim, Wohlforth utiliza o argumento de Layne para demonstrar que a unipolaridade não gerou uma pressão sistêmica que movesse o Sistema Internacional de volta a multipolaridade, uma vez que nenhum país (ou conjunto de países) demonstrou possuir as capacidades agregadas necessárias para representar um contrapeso na balança de poder estadunidense no imediato pós-Guerra Fria.

Todavia, quando se amplia esse debate para o ciberespaço, existe a possibilidade de que haja certa distribuição de poder entre Estados e, até mesmo, para atores não-estatais, o que poderia gerar certo grau de multipolaridade. Klimburg e Faesen (2018) argumentam que o ciberespaço é administrado por diversos atores, como a sociedade civil, o setor privado e entes governamentais. Para os autores, entretanto, os agentes governamentais representam aqueles que cada vez mais possuem uma postura assertiva no domínio cibernético, postura essa "que se encaminha para uma redistribuição de poder na qual os Estados não estão apenas competindo com outras partes interessadas, mas também entre si" (KLIMBURG; FAESEN, 2018, p. 01). Dessa forma, é possível compreender o ciberespaço como um agente democratizador de difusão de poder no Sistema Internacional, tendo em vista que Estados revisionistas e atores não-estatais como o setor financeiro, empresas de segurança e, até mesmo, indivíduos, podem obter destaque, poder e influência nesse domínio, alterando o *status quo* vigente (pelo menos no ciberespaço).

Outra possível forma de difusão de poder no Sistema Internacional ocorre por meio do poder exercido no espaço cibernético. Carr (2001, p. 143) divide o poder político em três categorias: poder militar, poder econômico e poder sobre a opinião. De acordo com o autor, o poder militar não representa apenas um instrumento, mas um fim em si mesmo, pois é essencial para a sobrevivência do Estado. Sobre o poder econômico, o autor discute como esse sempre foi necessário para obter progresso e desenvolvimento tecnológico,

sendo inclusive capaz de proporcionar o poder militar. Por fim, Carr considera o poder sobre a opinião como essencial, uma vez que a propaganda também pode ser utilizada como instrumento de política.

De forma a expor sua visão sobre o conceito de poder, Morgenthau (2003) o diferencia de influência. Para o autor, poder constitui a capacidade de fazer com que o outro aja de acordo com os seus interesses, ao passo que a influência significa a capacidade de fazer com que o outro escute seu conselho e, possivelmente, aja. Conforme Morgenthau, a principal diferença entre os dois termos se encontra no fato de que, caso o ator decida não agir após receber a influência, se o ator influenciador for detentor de poder este poderá forçar tal ação a ocorrer. Ainda sobre o poder, Morgenthau (2003, p. 51) destaca que este diz respeito ao "controle do homem sobre as mentes e ações de outros homens". De maneira mais específica, sobre o poder político, o autor discorre sobre como este consiste em "uma relação entre os que exercem poder e aqueles sobre os quais ele é exercido" (MORGENTHAU, 2003, p. 51).

Similar ao poder político de Morgenthau, onde há uma relação entre quem exerce poder e aquele sobre o qual o poder é exercido, Weber (1978, p. 53) define poder como "a probabilidade de que um ator dentro de uma relação social estará em posição de realizar sua própria vontade apesar da resistência, independentemente da base sobre a qual esta probabilidade repousa". Segundo Warren (1992), apesar do conceito de Weber não ser universalmente aceito, dois elementos-chave são replicados em quase todas as definições de poder: a compreensão do poder como uma expressão das vontades e capacidades de indivíduos e a distinção entre relações de poder e outras relações sociais em termos de conflito de interesse entre indivíduos (WARREN, 1992, p. 20).

Assim como outros conceitos importantes para o desenvolvimento desse trabalho (como ciberespaço, segurança cibernética, defesa cibernética, entre outros), o conceito de poder não possui definição única ou amplamente aceita. Nye (2010) discorre sobre como o poder, apesar de ser bastante utilizado na literatura, é um conceito elusivo e difícil de se definir. O autor argumenta que, por ser um conceito contestado, não existe uma definição comum aceita por todos que usam a palavra e, além disso, a definição utilizada reflete sempre os interesses e valores daquele que a define (NYE, 2010). Keohane e Nye (1977)

apontam que o poder é constituído pela habilidade de um ator conseguir fazer com que outros atores façam algo que não fariam normalmente. Nesse sentido, os autores discutem a questão da interdependência assimétrica. Diferentemente de autores realistas como Carr e Morgenthau que, usualmente, consideram atores como detentores de poder, Keohane e Nye discutem a possibilidade do poder estar presente não em um ator específico, mas sim na relação assimétrica de dependência entre um ator e outro.

O poder cibernético, por estar vinculado ao ciberespaço, possui características específicas e capacidade de impacto em diversos cenários. Willett (2019, p. 87) ao discorrer sobre a importância do poder cibernético, destaca que este não é simplesmente militar, mas sim multifacetado. Conforme o autor, pontos como a segurança cibernética dos serviços financeiros de um Estado e esforços em pesquisa e desenvolvimento são primordiais para o poder econômico e estão interligados ao poder cibernético. Da mesma forma, o suprimento de energia de Estados é fundamental para manter a segurança. Além disso, o autor ainda destaca as crescentes preocupações com processos eleitorais ao redor do mundo, estando o poder cibernético envolvido com todas essas questões e se mostrando como fator chave e estratégico para a integridade dos domínios nacionais (WILLETT, 2019, p. 87).

O poder cibernético, especialmente a partir do final do século XX e começo do século XXI, se torna item indispensável para a garantia de fornecimento de serviços básicos do Estado como o acesso à energia, água, luz, entre outros, como citado por Willett (2019). Maziero e Ayres Pinto (2019) definem o poder cibernético como aquele poder que é exercido no domínio cibernético. Todavia, os autores ressaltam que, apesar de o poder cibernético ser exercido no ciberespaço, "suas consequências e interações não se limitam a este espaço" (MAZIERO; AYRES PINTO, 2019, p. 4). Kuehl oferece uma definição mais completa do termo. Para o autor, o poder cibernético consiste na "habilidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os domínios operacionais e através de instrumentos de poder" (KUEHL, 2009, p. 12). O autor ainda especifica que sua definição é mais ampla para realçar a sinergia do poder cibernético e a integração dele com outras formas e instrumentos de poder existentes (KUEHL, 2009, p. 12).

De forma a realizar uma discussão comparativa entre ciberespaço e poder cibernético, Kuehl (2009) destaca que, ao passo que o ciberespaço simplesmente "é" (ou seja, simplesmente existe), o poder cibernético é uma medida da capacidade de usar o ciberespaço. O autor destaca alguns fatores necessários para a utilização do poder cibernético, como a tecnologia e fatores organizacionais. Similar a isso, Morgenthau (2003, p. 215) discorre - especialmente sobre países asiáticos - que nações com espaço geográfico considerável, recursos naturais, mão de obra disponível, tecnologia, capacidade industrial, educação e ciência poderiam, no futuro, fazer parte de uma possível redistribuição de poder no cenário internacional.

O que era discutido por Morgenthau de fato se concretizou com a ascensão de países como China, Índia, Coreia do Sul, entre outros. Sobre a tecnologia, Kuehl (2009) a coloca como fator óbvio para a utilização do domínio cibernético porque a capacidade de entrar no ciberespaço é o que permite a utilização dele por atores. Todavia, a tecnologia está em constante mudança e atualização. Portanto, atores estatais e não-estatais que queiram exercer poder no ciberespaço precisam ser capazes de superar tecnologias antigas de forma a conseguir implementar e utilizar tecnologias novas para, então, obter vantagens (KUEHL, 2009).

A importância dos fatores organizacionais no empreendimento do poder cibernético é discutida por Kuehl. Segundo o autor, ao serem criadas, organizações refletem "os propósitos e os objetivos humanos, e suas perspectivas sobre a criação e uso do poder cibernético serão moldadas pela missão da organização, seja ela militar, econômica ou política" (KUEHL, 2009, p. 38). Diante desse cenário, percebe-se que o poder cibernético poderá ser utilizado por aquele ator que consiga dominar (e que possua acesso) a determinadas tecnologias, seja esse ator estatal ou não. Ademais, também se verifica que o poder cibernético pode ser utilizado de diferentes formas, o que significa que esse poder varia de acordo com o que aquele que o exerce possui como objetivo.

A discussão realizada por Nye (2010) possui pontos em comum com aquela apresentada por Kuehl (2009): ambos autores destacam capacidades (recursos) e a importância do componente humano na utilização do poder. Especificamente sobre o poder cibernético, Nye (2010, p. 3) argumenta que

esse conceito é baseado em um conjunto de recursos relacionados tanto à criação e ao controle como à comunicação de informações eletrônicas e de computador (infraestrutura, redes, software e habilidades humanas). Sobre formas de comportamento, Nye (2010, p. 4) aponta que o poder cibernético é representado pela capacidade de se obter resultados preferidos via recursos de informação do ciberespaço interconectados eletronicamente. Assim, torna-se perceptível que, mesmo na discussão de poder cibernético de Nye, existem pontos em comum com as definições tradicionais de poder expostas com base em Carr, Morgenthau e Weber, como a capacidade de um ator conseguir resultados preferidos.

De maneira a relacionar o Sistema Internacional e o ciberespaço, verifica-se que o funcionamento do domínio cibernético desafia diretamente conceitos securitários clássicos. Isso ocorre devido às características inerentes do ciberespaço, como a desterritorialização e a fluidez, que fazem com que conceitos tradicionalmente estabelecidos precisem ser revisitados para que sejam realizadas as adaptações necessárias para utilizá-los corretamente no ambiente cibernético (OLIVEIRA; ROCHA; BOSSO, 2019, p. 2), como é o caso dos conceitos Segurança e Defesa.

De forma a retomar a discussão acerca da ampliação da agenda de segurança no pós Guerra Fria, tem-se o conceito de segurança humana, que apesar de estar presente na carta constitutiva da Organização das Nações Unidas (1945) e nos demais instrumentos de direito internacional com foco em indivíduos, passa a ser amplamente utilizado a partir da década de 1990, unindo questões referentes ao bem-estar, direitos e proteção individual. Tadjkbash e Chenoy (2007) levantam os questionamentos "segurança para quem?" e "para quê?". Os autores discorrem sobre o conceito de segurança humana, onde o indivíduo se torna tanto o amor final a ser levado em consideração como o foco da análise. A segurança do indivíduo, portanto, se torna o objetivo final e os instrumentos e atores estariam subordinados a isso. Esse conceito não explica as ameaças em si, mas reconhece o surgimento de novas ameaças junto à interdependência (TADJKBASH; CHENOY, 2007).

Considerando que a concepção tradicional de segurança enfatiza a integridade territorial e a independência nacional como os valores primários que precisam ser protegidos, a segurança humana diz respeito, em primeiro

lugar, à segurança e ao bem-estar de todas as pessoas em todos os lugares - em suas casas, empregos, ruas, comunidades e ambiente. O relatório do Programa das Nações Unidas para o Desenvolvimento (PNUD), de 1994, atribui a segurança humana em dois aspectos principais: *freedom from want e freedom from fear*. O primeiro está ligado a manter as pessoas a salvo de ameaças crônicas, pobreza, doenças infecciosas e degradação ambiental. O segundo se relaciona a proteger as pessoas de mudanças súbitas e nocivas dos padrões da vida cotidiana, como conflitos, violência e crime (MOSTAFAVI, 2009). Ademais, a segurança é distribuída em sete dimensões: econômica, alimentar, sanitária, ambiental, pessoal, comunitária e política (OLIVEIRA, 2009).

Como dito anteriormente, a ampliação da agenda de segurança passou a ocorrer a partir dos anos 1980. Com essa ampliação e uma maior utilização do termo "segurança nacional", a segurança de indivíduos, sociedades e outras questões passaram a pesar na agenda de segurança. Portanto, é interessante destacar que o termo segurança deixa de ser restrito ao mundo militar e passa a abordar questões como bem-estar econômico, pautas ambientes e, mais recentemente, questões que envolvem o espaço cibernético.

O presente capítulo buscou apresentar a discussão teórico-conceitual necessária para o desenvolvimento da pesquisa. Foram explorados conceitos basilares para a dissertação como governança; governança securitária, bem como foi explorada a situação da segurança e defesa no ambiente das relações internacionais e a questão referente ao poder e poder cibernético. Como será visto no próximo capítulo específico sobre Segurança, Defesa e Segurança Cibernética e Defesa Cibernética, a partir do momento em que a discussão sobre os termos Segurança e Defesa é transposta para o ciberespaço, as definições se tornam menos claras e mais fluidas. Conforme Pagliari, Ayres Pinto e Viggiano (2020, p. 153): "essa separação - especificamente, na área cibernética - é feita por uma linha tênue que em muitos momentos se desvanece, sendo difícil determinar ações de proteção específicas para cada tipo de ameaça e quem seriam os seus responsáveis diretos". O que se espera que o próximo capítulo seja útil ao constante debate acadêmico sobre a evolução da Segurança e Defesa Cibernética.

3 SEGURANÇA CIBERNÉTICA E DEFESA CIBERNÉTICA

Como introduzido ao final do capítulo anterior, as definições de Segurança e Defesa, quando transpostas para o ciberespaço, se tornam mais fluidas e menos claras. Além disso, junta-se o fato de que Defesa Cibernética e Segurança Cibernética são termos relativamente recentes e que não possuem definições únicas ou consensuais entre os autores que os discutem. Como será explorado ao longo deste capítulo, cientistas, organizações e Estados discorrem sobre a temática de cibernética e voltam seus esforços para definir esses conceitos, seja por meio de pesquisas científico-acadêmicas, seja por meio de documentos institucionais, ou documentos oficiais, como políticas de Defesa, por exemplo. O que se espera, ao decorrer do capítulo, é que, por meio de revisão bibliográfica e análise documental, seja possível identificar se é factível ou não diferenciar conceitualmente Segurança e Defesa no espaço cibernético. Todavia, antes de adentrar a discussão sobre Segurança e Defesa Cibernética, é realizada uma seção específica sobre os termos Segurança e Defesa.

3.1 SEGURANÇA E DEFESA

Antes de aprofundar a discussão acerca dos termos que fazem parte do objeto de pesquisa deste trabalho ao longo do capítulo - Defesa Cibernética e Segurança Cibernética -, é necessário diferenciar, a partir de revisão bibliográfica e documental, os próprios termos Defesa e Segurança. A diferença central entre Segurança e Defesa gira em torno do debate sobre atuação interna e externa, no qual agentes estatais de Segurança Pública são responsáveis pela segurança interna do país, ao passo que os agentes de Defesa Nacional são responsáveis pela defesa externa, ou seja, responsáveis por lidar com ameaças oriundas de fora do território nacional. Julga-se útil a elaboração de um quadro com a definição dos conceitos por parte dos Estados em análise antes de os explorar, de maneira a tornar a visualização e entendimento dos conceitos melhor.

Quadro 3 - Segurança e Segurança Nacional para Estados Unidos e Reino Unido

País	Definição de Segurança	Definição de Segurança Nacional
Estados Unidos	1. Medidas tomadas por uma unidade, atividade ou instalação militar para se proteger contra todos os atos destinados a, ou que possam prejudicar sua eficácia. 2. Condição que resulta do estabelecimento e manutenção de medidas de proteção que garantam um estado de inviolabilidade de atos ou influências hostis. 3. No que diz respeito ao material classificado, a condição que impede o acesso de pessoas não autorizadas a informação oficial tutelada no interesse da segurança nacional.[11]	Um termo coletivo que abrange a defesa nacional e as relações exteriores dos Estados Unidos com o objetivo de obter: 1. Uma vantagem militar ou de defesa sobre qualquer nação estrangeira ou grupo de nações; 2. Uma posição favorável nas relações exteriores; ou 3. Uma postura de defesa capaz de resistir com sucesso a ações hostis ou destrutivas de dentro ou de fora, aberta ou dissimulada.[12]
Reino Unido	Apesar da Estratégia Nacional de Segurança (National Security Strategy) do Reino Unido mencionar "security" 517 vezes, o documento não apresenta uma definição do termo.	O primeiro objetivo é proteger nosso povo - em casa, em nossos territórios ultramarinos e no exterior, e proteger nosso território, segurança econômica, infraestrutura e modo de vida. O segundo objetivo é projetar nossa influência global - reduzindo a probabilidade de ameaças que se materializem e afetem o Reino Unido, nossos interesses e os de nossos aliados e parceiros. O terceiro objetivo é promover nossa prosperidade - aproveitando oportunidades, trabalhando de forma inovadora e apoiando a indústria do Reino Unido.[13]

Fonte: elaborado pelo autor com base em Estados Unidos (2021); Reino Unido (2015).

[11] [Tradução própria]. No original, lê-se: *1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.*

[12] [Tradução própria]. No original, lê-se*: A collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: a. A military or defense advantage over any foreign nation or group of nations; b. A favorable foreign relations position; or c. A defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert.*

[13] [Tradução própria]. No original, lê-se: *Objective 1 is to protect our people – at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life. Objective 2 is to project our global influence – reducing the likelihood of threats materialising and affecting the UK, our interests, and those of our allies and partners. Objective 3 is to promote our prosperity – seizing opportunities, working innovatively and supporting UK industry.*

No caso do Reino Unido foram explorados os documentos A Strong Britain in an Age of Uncertainty: The National Security Strategy e National Security Strategy and Strategic Defence and Security Review, ambos de 2015. No primeiro, a palavra "security" é encontrada 239 vezes, no segundo, 517. No entanto, nenhum dos documentos fornece uma definição para o conceito de Segurança e o governo não disponibiliza nenhum tipo de glossário ou dicionário específico para as Forças Armadas ou para termos militares em geral. É interessante pensar que, talvez, não definir o termo seja uma opção calculada pelo Reino Unido, uma vez que, não estando preso a uma definição estanque, o Estado não limita suas possibilidades de ação no âmbito de Segurança.

A discussão específica sobre segurança, portanto, acaba sendo limitada aos Estados Unidos porque o Reino Unido, em sua Estratégia Nacional de Segurança, não fornece uma definição do conceito. A definição estadunidense de Segurança, apesar de colocar a segurança como "condição resultante do estabelecimento e manutenção de medidas de proteção que garantem um estado de inviolabilidade de atos ou influências hostis" (UNITED STATES, 2021, p. 150), é bastante singular. Diferentemente do que usualmente é exposto sobre Segurança (que é a ligação do termo com a sensação de estar seguro), os Estados Unidos elencam que a Segurança pode significar, também, ações concretas empreendidas por unidades militares para se proteger contra possíveis danos.

Buzan (1991, p. 100) afirma que a Segurança Nacional "pode ser vista principalmente em termos de proteção dos componentes do Estado de ameaças e interferências externas". A definição de Buzan vai de encontro às definições dos dois países. No caso estadunidense, por exemplo, é colocado que a Segurança Nacional representa, entre outras coisas, uma postura de defesa "capaz de resistir com sucesso a ações hostis ou destrutivas de dentro ou de fora". Ou seja, os Estados Unidos elencam a capacidade de defesa contra ações de atores externos como parte essencial da Segurança Nacional.

Cavagnari Filho (1994, p. 43), conforme citado por Herz (2010, p. 601), define Segurança Nacional da seguinte forma:

> Segurança nacional é a garantia relativa dos interesses nacionais no nível nacional e também nas relações internacionais. A dimensão militar da segurança deriva do alcance das Forças Armadas na defesa desses interesses diante das ameaças que justificam seu uso e da capacidade do inimigo que gera essas ameaças. Esse aspecto enfatiza as diferenças entre países[14].

A partir da definição de Cavagnari (1994), é possível identificar a segurança nacional como a garantia de segurança do Estado (assim como visto nos casos de Estados Unidos e Reino Unido), sendo as Forças Armadas a instituição garantidora dessa segurança no sistema internacional. Consoante Rudzit e Nogami (2010), a Segurança Nacional só pode ser interpretada como um problema político a partir do momento em que se tem uma ideia "razoavelmente clara sobre a natureza de uma ameaça e as vulnerabilidades do objeto ao qual as ameaças são dirigidas" (RUDZIT; NOGAMI, p. 6, 2010). Para os autores, a distinção entre ameaças e vulnerabilidades revela a significativa divisão existente em políticas de Segurança Nacional, uma vez que países podem ter como estratégia reduzir suas inseguranças por meio da diminuição das vulnerabilidades identificadas, ou por meio do enfraquecimento das fontes de ameaça (RUDZIT; NOGAMI, 2010).

Um ponto interessante na definição de Segurança Nacional dos Estados Unidos é que o país qualifica o conceito como "um termo coletivo que abrange a defesa nacional", além de destacar vantagens militares e/ou de defesa sobre qualquer nação estrangeira ou grupo de nações como parte da Segurança Nacional. Ou seja, para os Estados Unidos, o conceito de Segurança Nacional abrange o caráter militar que, antes do fim da Guerra Fria, estava sob o guarda-chuva do conceito de Segurança, que atualmente também lida com questões econômicas, ambientais, sociais, entre outras, como visto no capítulo anterior. Algo similar é discutido por Buzan et al. (1998, p. 29) quando os autores argumentam que a Segurança Nacional pode "funcionar de maneira a silenciar opositores e a fornecer àqueles que a detém inúmeras oportunidades para explorar ameaças para fins domésticos".

---

[14] [Tradução própria]. No original, lê-se: "*national security is the relative guarantee of national interests within the state and in inter-state relations. The military dimension of security derives from the reach of the armed forces in defence of these interests in face of threats that justify their use and of the capacity of the enemy that generates these threats. This aspect stresses the differences between countries*".

No caso do Reino Unido, é caracterizado como Segurança Nacional a capacidade de proteger o povo tanto em território nacional, ultramarino, ou no exterior. O Estado inclui na sua definição um objetivo bastante similar ao estadunidense: a vontade de projetar sua influência no âmbito internacional, com o intuito de reduzir as ameaças ao país. Contudo, o último objetivo destacado pelo Reino Unido é bastante singular: o documento salienta a promoção da prosperidade econômica como um objetivo de Segurança Nacional, algo que não é visto no caso estadunidense.

Segurança, conforme Cepik (2001), representa uma condição relativa de proteção na qual se tem a capacidade de neutralizar ameaças contra a existência de alguém ou de alguma coisa, similar a definição de Segurança dos Estados Unidos. Por outro lado, de acordo com o autor, a segurança nacional é entendida como uma condição de proteção coletiva e individual dos membros de uma sociedade contra ameaças plausíveis a sua sobrevivência e autonomia. A definição do Reino Unido, assim como a de Cepik (2001), coloca a proteção da população como objetivo prioritário da segurança nacional. Com a ampliação da agenda de segurança no período pós Guerra Fria, a segurança nacional passou a se preocupar tanto com ameaças externas como internas (além de terem sido incluídas ameaças não-estatais), diferentemente do que ocorria durante a Guerra Fria, quando a agenda de segurança estava focada em ameaças militares externas.

Sobre o conceito de Segurança, ressalta-se que as vezes ele também é visto como um estado, ou seja, como a sensação de sentir segurança (WINTER, 2006; CARDOSO et. al, 2013; SANTOS, 2016). Um exemplo hipotético disso seria a situação da população de uma determinada região ou Estado que 1. não possui inimigos, criminalidade interna ou ameaças ou 2. possui capacidades de se defender contra qualquer ameaça iminente ao ponto de não precisar se preocupar com possíveis inseguranças. Wolfers (1952) discorre sobre como o valor da segurança varia de Estado para Estado. Isso porque, segundo o autor, existem Estados que por se sentirem tão insatisfeitos com o *status quo*, estão dispostos a passar por inseguranças na tentativa de alterar sua posição no Sistema Internacional.

Nesse sentido, Wolfers (1952) enxerga a Segurança como algo que um Estado pode ter mais ou menos, bem como pode desejar ter em maior ou

menor quantidade (BALDWIN, 1997). Brodie (1950), por sua vez, expõe que a visão do conceito de Segurança como algo que se pode ter mais ou menos não é amplamente aceita. Conforme o autor, não é possível ser parcialmente seguro: "se estivermos seguros pela metade, não estamos seguros de forma alguma" (BRODIE, 1950, p. 5). A visão de Segurança de Brodie, apesar de publicada na metade do século passado, continua atual. Atualmente, nem mesmo China, Estados Unidos, França, Reino Unido e Rússia, que são membros permanentes do Conselho de Segurança das Nações Unidas, se consideram seguros ou invencíveis no Sistema Internacional. O que vemos, na verdade, é o preparo e investimento contínuo de tais países nas áreas de Segurança e Defesa para lidar com ameaças insurgentes, como as ameaças cibernéticas.

Após a reflexão sobre Segurança, será realizada discussão sobre Defesa, com o intuito de se entender as principais diferenças entre os termos. Ressalta-se que não será utilizado quadro para explorar as definições de Defesa porque Estados Unidos e Reino Unido não possuem uma definição específica de defesa divulgada em documentos oficiais. É importante enfatizar que a não definição do termo por Estados Unidos e Reino Unido é uma informação a ser levada em conta porque, uma vez que os países não definem o termo, este não é restrito ou limitado, o que permite aos Estados o utilizarem de maneiras distintas ao longo do tempo.

Costa (1999) diferencia Segurança e Defesa da seguinte forma: segurança como um estado e defesa como um ato. Nesse sentido, o autor destaca que as questões relacionadas à segurança devem ser precedentes ao estabelecimento de uma política de Defesa. Mas o que significa a preocupação com segurança ser precedente àquela com a defesa? Significa, resumidamente, que o Estado deve levantar os pilares que servirão para garantir a segurança de seu território, soberania e população para, após isso, articular formas de defesa, no caso de seus pilares serem ameaçados (COSTA, 1999).

Os Estados Unidos divulgaram apenas o sumário de sua Estratégia Nacional de Defesa (2018), portanto, é impossível afirmar se ao longo do documento completo o país define ou não defesa. Entretanto, no sumário o termo não é definido. Todavia, no sumário disponibilizado, os Estados Unidos

colocam certos objetivos de Defesa que o país possui, como por exemplo: "defender a pátria de ataques"; "dissuadir os adversários de agredir nossos interesses vitais"; "manutenção de equilíbrios de poder regionais favoráveis nas regiões Indo-Pacífica, Europa, Oriente Médio e Hemisfério Ocidental"[15] (UNITED STATES, 2018, p. 4). Apesar do país não divulgar sua definição de defesa, os objetivos usuais como defesa territorial e dissuasão de ataques estão presentes.

No entanto, os Estados Unidos adicionam aos seus objetivos de defesa algo bastante singular: a manutenção da balança de poder em regiões que o país considera estratégicas, como o Indo-Pacífico, a Europa, o Oriente Médio e o Hemisfério Ocidental. Como discutido anteriormente por meio de Morgenthau (2003), a manutenção da balança de poder significa, basicamente, um esforço de forças (Estados) para manter o equilíbrio de poder no Sistema Internacional e garantir que nenhum Estado acumule poder demais sozinho.

O que é enfatizado pelos Estados Unidos é que eles estão presentes militarmente ao redor do mundo para garantir que não haja nenhuma mudança radical em balanças de poder regionais que possam vir a afetá-los (UNITED STATES, 2018, p. 4). É possível inferir, a partir da exposição sobre a balança de poder por parte dos Estados Unidos em seu documento, que o país está presente nas diversas regiões do globo para garantir que o *status quo* vigente, o qual os favorece, seja mantido. Nesse sentido, torna-se perceptível que o país não está preocupado se a balança está irregular para Estado X na Europa ou para Estado Y no Oriente Médio, mas sim está preocupado em garantir que não haja nenhuma mudança nessas regiões que venha a afetar a balança que é favorável aos próprios Estados Unidos.

Os Estados Unidos, apesar de não definir especificamente o termo "Defesa" em seus documentos oficiais, define termos ligados à Defesa, como os termos "defesa ativa" e "defesa passiva". A defesa ativa corresponde ao emprego de ações ofensivas limitadas e contra-ataques para negar uma área ou posição contestada ao inimigo, ao passo que a defesa passiva é referente às medidas tomadas pelo país para que se reduza a probabilidade e minimize

---

[15] [Tradução própria]. No original, lê-se: *Defending the homeland from attack; Deterring adversaries from aggression against our vital interests; Maintaining favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere*.

os efeitos de danos causados por ações hostis (ESTADOS UNIDOS, 2021). Além disso, ressalta-se que os Estados Unidos definem outros termos vinculados à Defesa como defesa aérea; defesa aeroespacial; defesa cibernética; defesa química, biológica, radiológica e nuclear, entre outros.

Assim como ocorreu com o termo Segurança, Defesa também não foi definido pelo Reino Unido na *National Security Strategy and Strategic Defence and Security Review* de 2015, apesar da palavra "*defence*" ser encontrada 236 vezes no documento. No entanto, o Reino Unido (2015) destaca algumas missões de Defesa estabelecidas pela nação, como, por exemplo: a defesa e contribuição para a segurança e resiliência do Reino Unido e dos territórios ultramarinos; a dissuasão de ataques; a defesa dos espaços aéreo, marítimo, terrestre e cibernético; reforçar a segurança internacional e a capacidade coletiva dos aliados da nação, parceiros e instituições multilaterais.

Assim como os Estados Unidos, o Reino Unido não apresenta uma definição explícita do termo Defesa. Entretanto, o país discorre sobre como a Defesa contribui de forma significativa com o apoio dos objetivos políticos do governo em influenciar o comportamento de qualquer grupo, nação ou Estado que ameace os interesses do Reino Unido. Função essa que é realizada por meio da análise de ameaças e, consequentemente, pelas recomendações apropriadas para lidar com as ameaças em questão. Entre as principais contribuições da Defesa apontadas pelo Reino Unido estão as estratégias de dissuasão e coerção aplicadas de maneira integrada. O país destaca, também, que como um dos principais instrumentos disponíveis ao governo, a Defesa representa um papel único ao proteger e promover três interesses nacionais fundamentais: soberania, segurança e prosperidade. Os quais incluem a proteção da população britânica, do seu território e da infraestrutura crítica (REINO UNIDO, 2021).

O fato de Estados Unidos e Reino Unido não definirem o termo Defesa, apesar de discorrerem sobre ações vinculadas ao termo defesa ou sobre outros termos relacionados à defesa (como defesa cibernética ou defesa aérea) é bastante emblemático. Isso porque, uma vez que os países não adotem definições específicas sobre esse conceito, não existe um escopo de atuação que limite até onde pode ir a atuação desse país para realizar ações vinculadas à defesa. Essa não-definição pode servir ao país para permitir

ações que talvez que não seriam permitidas se houvesse determinada limitação, ao mesmo tempo que essa não-definição pode servir como escape para atuações indevidas de Estado como violações de direitos humanos, por exemplo (BREWER, 2008).

O conceito de Defesa, diferentemente do conceito de Segurança, é menos alterado ao longo do tempo. Entre as definições de Defesa disponíveis pelo Dicionário Oxford, por exemplo, está a "proteção contra ataques inimigos". Apesar de ser uma definição bastante simples, ela sintetiza o que é Defesa: que é a proteção do território de um Estado ou nação, de sua população e sua soberania em relação a atores externos. De forma alguma o fato do conceito de Defesa se manter ao longo do tempo deve significar que Estados irão utilizá-lo apenas de uma forma ou outra. É necessário ter em mente que esse termo é condicionado e empregado por diferentes Estados com base em distintas ameaças, ambições e capacidades, e isso permite entender que diferentes contextos resultarão em distintas formas de Defesa.

De acordo com Átria (2003), a Defesa - e em especial as Forças Armadas - é responsável por oferecer a capacitação militar em termos "materiais, doutrinários, científicos e tecnológicos, bélicos e de recursos humanos" (ÁTRIA, 2003, p. 18). Portanto, conforme o autor, o conceito de Defesa deve abarcar a preparação de militares desde o nível mais básico (doutrinário) ao nível mais avançado (bélico), que seria, de fato, a atuação do militar em situação de guerra ou conflito. Por sua vez, Amorim (2012) destaca que o objetivo principal da defesa é evitar, com base em capacidades militares adequadas, que ocorram agressões ao patrimônio de determinado país ou ações que afetem, mesmo que de maneira indireta, os interesses nacionais.

Como discutido na introdução da pesquisa, uma das principais diferenças entre Segurança e Defesa se encontra no caráter de atuação interno ou externo dos. Ao passo que forças de segurança - ou autoridades policiais - devem estar preparadas para aplicar a lei e manter a ordem interna do Estado, as Forças Armadas devem estar preparadas para lidar com ameaças externas, com a manutenção da soberania do Estado e para manter a integridade territorial de seu país. Dessa forma, as autoridades de Segurança são responsáveis por manter o ordenamento interno do país e as Forças Armadas

são responsáveis por lidar com ameaças externas e por estar preparadas para uma eventual situação de guerra ou conflito.

Posto isso, no presente trabalho o conceito de Segurança é compreendido tanto como a capacidade de um Estado (por meio de suas autoridades policiais) de manter a ordem interna, como também é compreendido como a sensação da população de estar segura em seu país ou região. O conceito de Defesa, por sua vez, é compreendido como a capacidade das Forças Armadas de um Estado para lidar com qualquer ameaça externa que possa querer ferir sua soberania, integridade territorial, sua população ou os interesses nacionais de determinado país.

Quando se pensa na atuação de atores de Segurança e Defesa, a diferença pode parecer clara: ao passo que atores de Segurança são responsáveis por lidar com ameaças internas, atores de Defesa devem lidar com ameaças externas (oriundas de fora do território nacional). Existem, contudo, casos específicos nos quais atores de Defesa podem atuar internamente, como, por exemplo, em ações subsidiárias ou operações de Garantia da Lei e da Ordem (GLO), como é o caso do Estado brasileiro (BRASIL, 1999). No entanto, quando se pensa na atuação desses mesmos atores no ciberespaço, a discussão se torna mais complexa e os termos menos claros.

Apesar da distinção de atuação entre atores de Segurança e Defesa parecer clara (pelo menos nos domínios tradicionais como ar, mar e terra), a discussão que ocorre ao redor do significado dos termos Segurança e Defesa ainda não alcançou um consenso. Como destacado por Fernandes (2012), o campo de Estudos Estratégicos e Estudos de Defesa ainda não possui consenso sobre muitos conceitos importantes (como Segurança, Defesa, Poder), o que permite que autores utilizem esses conceitos livremente - e de formas distintas. No mesmo sentido, Baldwin (1997) argumenta que, mesmo com o uso generalizado do termo Segurança por acadêmicos e políticos nas últimas décadas, houve pouca preocupação em explicar o conceito de fato. Nesse sentido, na presente discussão o que se propõe a fazer é pensar a Segurança e a Defesa de forma a contribuir com a discussão sobre a temática e a fornecer possíveis interpretações para os termos relacionando-os com o domínio cibernético.

3.2 SEGURANÇA CIBERNÉTICA

A Segurança Cibernética, de acordo com Lewis (2006), envolve a proteção das redes de computador e das informações contidas nessas redes contra danos, interrupções ou entradas malignas. Amoroso (2006) aprofunda um pouco mais a discussão. Para o autor, a Segurança Cibernética envolve tanto a redução de riscos contra ataques maliciosos à *softwares*, computadores e redes, como a inclusão de ferramentas utilizadas para detectar invasões, interromper vírus, bloquear acessos maliciosos, impor autenticação e habilitar comunicações criptografadas. Nesse sentido, começa-se a perceber que as definições de Segurança Cibernética vão desde o mais simples, como quando autores discorrem sobre a proteção de redes e informações, às situações mais complexas como ferramentas específicas para detectar invasões, interromper vírus e habilitar comunicações criptografadas, por exemplo.

Com o intuito de fornecer as informações de forma clara aos leitores, são elaborados dois quadros ao longo do capítulo: o primeiro contendo definições de Estados Unidos, Reino Unido e acadêmicos para Segurança Cibernética e o segundo, contendo as definições para Defesa Cibernética. Ressalta-se que a Organização do Tratado do Atlântico Norte (OTAN) não define Segurança Cibernética, define apenas Defesa Cibernética Ativa. O que se espera é que a utilização dos quadros ajude o leitor a compreender as diferentes visões sobre os conceitos. Ao longo da leitura do quadro a seguir, será possível identificar diferentes interpretações sobre Segurança Cibernética.

Quadro 4 - Definições de Segurança Cibernética

Autor	Definição
Estados Unidos (2020).	"A atividade ou processo, habilidade ou capacidade, ou estado pelo qual os sistemas de informação e comunicação, bem como as informações neles contidas, são protegidos e/ou defendidos contra danos, uso não autorizado ou modificação, ou exploração."[16]

[16] [Tradução própria]. No original, lê-se: *The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.*

Reino Unido (2016).	"A proteção de sistemas conectados à internet (incluindo hardware, software e a infraestrutura associada), bem como os dados neles contidos e os serviços providos por eles, contra acesso não autorizado, dano ou uso indevido. Isso inclui danos causados intencionalmente pelo operador do sistema, ou acidentalmente, como resultado de não seguir os procedimentos de segurança ou ser manipulado a fazê-lo."[17]
Lewis (2006, p. 1)	"A segurança cibernética envolve a proteção de redes de computadores e das informações nelas contidas contra penetração e danos ou interrupções maliciosas."[18]
Cavelty (2010, p. 155).	"Refere-se a um conjunto de atividades e medidas (técnicas e não-técnicas), destinadas a proteger a "geografia real" do ciberespaço, bem como dispositivos, software - e as informações ou dados que estes contêm e comunicam -, de todas as possíveis ameaças."[19]
Von Solms e Van Niekerk (2013, p. 5).	"A segurança cibernética pode ser definida como a proteção do ciberespaço em si, das informações eletrônicas, das tecnologias da informação e comunicação que dão suporte ao ciberespaço, e dos usuários do ciberespaço em sua capacidade pessoal, social e nacional, incluindo quaisquer de seus interesses, tangíveis ou intangíveis, que sejam vulneráveis à ataques originados no ciberespaço."[20]
Souza (2013, p. 27).	"O combate e a prevenção dos chamados crimes cibernéticos na esfera da segurança pública."
Pelton e Singh (2015, p. 160)	"Métodos e ferramentas que podem ser usados para proteger a privacidade online de uma pessoa e para evitar ataques digitais em um computador, smartphone ou outros dispositivos eletrônicos."[21]

[17] [Tradução própria]. No original, lê-se: *The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.*

[18] [Tradução própria]. No original, lê-se: *Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.*

[19] [Tradução própria]. No original, lê-se: *It refers to a set of activities and measures, technical and non-technical, intended to protect the 'real geography' of cyberspace but also devices, software, and the information or data they contain and communicate, from all possible threats.*

[20] [Tradução própria]. No original, lê-se: *Cyber security can be defined as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace.*

[21] [Tradução própria]. No original, lê-se: *Methods and tools that can be used to protect one's online privacy and to prevent digital attacks on one's computer, smart phone, or other electronic device.s*

Bay (2016, p. 24)	“A segurança cibernética é uma questão securitária que abrange desde o nível do indivíduo contra ameaças cibernéticas até a sociedade como um todo.”[22]

Fonte: elaboração própria, com base nas fontes expostas na coluna “Autor”.

A partir do quadro acima, torna-se possível inferir que existem similaridades entre as definições apresentadas. A definição dos Estados Unidos resgata o conceito elaborado por Lewis (2006), o qual prevê a Segurança Cibernética como forma de proteção das redes de computador e das informações contidas nessas redes contra danos, interrupções ou entradas malignas. O Reino Unido, assim como os Estados Unidos, estabelece que a Segurança Cibernética será responsável pelas redes e dados/informações contidos no domínio virtual. Todavia, algo que o Reino Unido coloca em sua definição - e que não é exposto pelos Estados Unidos - é o caráter de proteção às infraestruturas críticas, as quais estão presentes no domínio físico.

Essa proteção às infraestruturas críticas destacada pelo Reino Unido também se relaciona diretamente com a definição de Cavelty (2010), a qual pressupõe que a Segurança Cibernética se destina a proteger a "geografia real" do ciberespaço, representada pela infraestrutura física que permite a existência do domínio cibernético. Entretanto, a autora adiciona em sua definição que a Segurança Cibernética é, em seu fim, a capacidade estatal de proteger o ciberespaço de "todas as possíveis ameaças" (CAVELTY, 2010, p. 155), o que se aproxima, também, da definição estadunidense de Segurança Cibernética, uma vez que os Estados Unidos igualmente salientam em sua definição que ela constitui capacidade estatal de proteger os seus sistemas e aquilo que neles está contido.

Por sua vez, Von Solms e Van Niekerk (2013) trazem uma variável importante ao pensarem a Segurança Cibernética como a "segurança pública" do ciberespaço. Os autores apontam para a proteção dos usuários do ciberespaço, seja em capacidade pessoal, social ou nacional (o que se relaciona diretamente com a definição estadunidense), incluindo quaisquer de seus interesses (VON SOLMS; VAN NIEKERK, 2013, p. 5). Souza (2013) faz parte da corrente de autores que consideram a Segurança Cibernética como

[22] [Tradução própria]. No original, lê-se: *Cybersecurity is a security matter which spans from the individual’s security against cyber threats to all of society*.

Segurança Pública; portanto, o dever desta - para o autor -, consiste no combate e na prevenção de crimes cibernéticos. O ponto de vista desses autores é bastante interessante porque, de acordo com a análise que eles apresentam sobre a Segurança Cibernética, ela seria equivalente à Segurança Pública dos domínios tradicionais, orquestrada, teoricamente, por organismos estatais da área de Segurança.

Conforme Bay (2016), a segurança cibernética é uma questão securitária que abrange desde o nível do indivíduo contra ameaças cibernéticas até a sociedade como um todo (como também é exposto por Von Solms e Van Niekerk quando estes destacam que a Segurança Cibernética precisa acontecer tanto em capacidade pessoal, social e nacional). Pelton e Singh (2015), por sua vez, estabelecem que a Segurança Cibernética representa os métodos e as ferramentas que podem ser utilizados para proteger a privacidade de uma pessoa online e, também, para evitar ataques digitais em um computador, *smartphone* ou outros dispositivos eletrônicos. Sobre a capacidade de Segurança Cibernética nos níveis pessoal e social, destacam-se esforços governamentais de incentivo ao aprendizado sobre questões cibernéticas, como ocorre nas escolas do Reino Unido.

Como é possível inferir a partir das definições estatais expostas no quadro, apesar de cada país optar por sua escolha de palavras, existem similaridades na definição de Segurança Cibernética de Estados Unidos e Reino Unido, bem como existem diferenças. Os Estados Unidos utilizam diversos substantivos para se referir ao tema, como atividade, processo, capacidade e estado de proteção e defesa. Se aproximando, dessa forma, das definições de Von Solms e Van Niekerk (2013), Lewis (2006), Cavelty (2010) e, até mesmo, de Souza (2013), no que diz respeito ao combate e prevenção de crimes cibernéticos, quando o país discorre sobre capacidades de Defesa contra uso não autorizado, modificações ou explorações. Além disso, com base no que é apresentado pelos Estados Unidos, é possível inferir que o Estado tem se preparado para atuar em diversas frentes dentro do âmbito daquilo que é entendido por Segurança Cibernética pelo Estado.

O Reino Unido, por sua vez, dá destaque inteiramente ao substantivo proteção. No entanto, a definição é similar à de Lewis (2006), que também destaca a proteção de redes de computadores e das informações neles

contidas. A definição do país também se aproxima da definição dos Estados Unidos no momento em que o Reino Unido salienta a proteção contra acesso não autorizado, dano ou uso indevido. Destaca-se que essas palavras, apesar de parecerem apenas parte da definição de um termo, são de extrema importância porque fazem parte de um possível discurso do que pode ou não ser realizado no ciberespaço por esses dois países. Os Estados Unidos, por exemplo, enfatizam a proteção e defesa como meios para proteger os seus sistemas e informações, assim como o Reino Unido.

Posto isso, a Segurança Cibernética é aqui compreendida como a capacidade de proteção dos sistemas conectados à internet e das informações e dados contidos nesses sistemas, bem como das camadas vinculadas ao ciberespaço, seja *hardware*, seja *software* ou *peopleware.* E, em um sentido mais amplo, a Segurança Cibernética representa a capacidade de assegurar o mantenimento da sociedade da informação de um país no ciberespaço.

Ressalta-se que, entre todas as definições sobre Segurança Cibernética aqui trabalhadas, nenhuma discorre sobre ações ofensivas no ciberespaço. O que pode significar que, para os autores em questão (inclusive os dois Estados em análise), a Segurança Cibernética deve focar, especialmente, em ações preventivas que sirvam para evitar a violação do ciberespaço e do conteúdo que nele existe. Ou, caso o ciberespaço acabe por ser violado, em ações de recuperação, mas não em ações ofensivas, como ataques cibernéticos, por exemplo.

3.3 DEFESA CIBERNÉTICA

Ao pensar sobre Defesa Cibernética, se pressupõe que o sentido lógico seria que, assim como a Defesa Nacional, a defesa do ciberespaço tivesse como objetivo o ato de lidar e deter ameaças advindas de fora do território nacional. Todavia, como demonstrado ao longo do trabalho (especialmente na seção sobre o ciberespaço), as fronteiras, barreiras, entradas e saídas do domínio cibernético não são estáticas como as fronteiras físicas. Portanto, realizar a atribuição de atores responsáveis por lidar com questões de Defesa Cibernética e Segurança Cibernética se torna um desafio tanto para acadêmicos como para os próprios aparatos do Estado, visto que ainda existe

uma neblina sobre o que é, de fato, considerado apenas Segurança ou Defesa no ciberespaço.

Libicki (2009) define que a Defesa Cibernética inclui tudo aquilo que é necessário para fazer com que atacantes não tenham sucesso em suas tentativas e não se beneficiem de seus esforços. A definição de Libicki é bastante ampla, pois apenas destaca que a Defesa Cibernética inclui tudo o que for necessário para garantir o não-sucesso dos atacantes, o que abre espaço para interpretação e subjetividade sobre o que pode ou não fazer parte do conceito, bem como expande a atuação do Estado para tudo o que for julgado necessário por ele para atingir seus objetivos.

A definição de Souza e Almeida (2016, p. 395) é um pouco mais detalhada do que a de Libicki. Os autores enfatizam que a Defesa Cibernética se refere a "ações operacionais, de caráter ofensivo, caracterizadas por ataques cibernéticos (neste sentido composto pela participação de elementos estatais)". Diferentemente das definições de Segurança Cibernética exploradas na seção anterior, aqui já se torna perceptível o caráter ofensivo do aparato estatal ao lidar com a defesa do ciberespaço, especificado pela utilização de ataques cibernéticos.

Devido a dificuldade de encontrar conceitos bem definidos ou estabelecidos sobre Defesa Cibernética para o desenvolvimento de Políticas e Estratégias de Defesa, Dewar (2014) sugere a utilização do conceito de Defesa Cibernética Ativa (conceito que também é utilizado pelo Reino Unido). Para o autor, a definição desse conceito se baseia em medidas proativas que vão além da detecção e análise das violações de segurança em tempo real e da mitigação de danos. Esse conceito serve, também, para cobrir contramedidas agressivas realizadas fora da rede na qual a vítima foi agredida.

Nesse sentido, por exemplo, caso o Estado X identifique que foi violado pelo Estado Y no ambiente cibernético, o Estado X pode recorrer a um ataque tradicional-físico para retaliar o Estado Y. Ressalta-se que, devido a dificuldade de se conseguir atribuir atos a atores no ciberespaço, para a realização de um ataque tradicional-físico como resposta a um ataque sofrido no âmbito do ciberespaço seria necessário haver absoluta certeza de quem, de fato, realizou tal delito, de forma a evitar uma resposta equivocada.

A seguir será exposto um quadro para o melhor entendimento do que é compreendido por Defesa Cibernética, contendo definições elaboradas por acadêmicos da área, bem como as definições utilizadas pelos dois Estados em análise nesta pesquisa. Como será visto, o Reino Unido se utiliza do mesmo conceito discutido por Dewar (2014), o qual entende a Defesa Cibernética como Defesa Cibernética Ativa.

Quadro 5 - Definições de Defesa Cibernética

País	Definição de Defesa Cibernética
Estados Unidos	Ações tomadas dentro do ciberespaço protegido para derrotar ameaças específicas que violam ou ameaçam violar as medidas de segurança do ciberespaço e incluem ações para detectar, caracterizar, combater e mitigar ameaças, incluindo *malware* ou atividades não autorizadas de usuários, e também a restauração do sistema para uma configuração segura.[23]
Reino Unido	A Defesa Cibernética Ativa (Active Cyber Defense – ACD) consiste em adotar medidas de segurança capazes de fortalecer uma rede ou sistema e torná-lo mais robusto contra ataques. Em um contexto não governamental, a Defesa Cibernética Ativa geralmente se refere à atuação de analistas de segurança cibernética no diagnóstico das ameaças às suas redes e na formulação e implementação de medidas proativas de combate ou defesa contra essas ameaças.
OTAN	Defesa cibernética ativa: A tomada de medidas defensivas proativas fora da infraestrutura cibernética protegida.
Libicki	A Defesa Cibernética inclui tudo o que é necessário para impedir que os invasores tenham sucesso e se beneficiem de seus esforços.[24]

[23] [Tradução própria] No original, lê-se: *Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration.*
[24] [Tradução própria]. No original, lê-se: *Cyberdefense includes everything required to keep attackers from succeeding and benefiting from their efforts.*

Dewar	A Defesa Cibernética Ativa é um método de alcançar a segurança cibernética baseado no desenvolvimento de medidas para detectar, analisar, identificar e mitigar ameaças de e para o ciberespaço em tempo real, combinado com a capacidade e recursos para tomar ações proativas ou agressivas contra agentes de ameaça nas redes domésticas desses agentes.[25]
Souza e Almeida	Ações operacionais, de caráter ofensivo, caracterizadas por ataques cibernéticos (neste sentido composto pela participação de elementos estatais).
Carvalho	O conjunto de ações realizadas no espaço cibernético para defender os sistemas e as informações.
Guedes et al.	Ato de defender o sistema crítico das TICs de um Estado. Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país.
Galinec, Možnik e Guberina	Detectar e fornecer respostas oportunas a ataques ou ameaças para que nenhuma infraestrutura ou informação seja adulterada.

Fonte: elaboração própria com base em Dewar (2014); Estados Unidos (2021); Libicki (2009); Reino Unido (2016); Souza e Almeida (2016); Guedes et. al (2017); Galinec; Možnik; Guberina (2017); Carvalho (2011).

Com base na tabela elaborada a partir das definições de Estados Unidos, Reino Unido e acadêmicos da área, pode-se verificar que, diferentemente das definições de Segurança Cibernética trabalhadas anteriormente, a Defesa Cibernética possui, como ponto central, ações ofensivas para se proteger no ciberespaço. Com exceção da definição de Libicki, todas as definições apresentadas são bastante diretas ao discorrer sobre o componente ofensivo da Defesa Cibernética. O Reino Unido, apesar de não usar o termo "ações ofensivas", utiliza medidas proativas de combate a ameaças. O que não é discutido pelo Reino Unido em seu conceito de Defesa Cibernética Ativa mas que é salientado por Dewar (2014) é que a Defesa Cibernética Ativa permite que um Estado atacado no domínio cibernético recorra a ataques tradicionais como forma de retaliação.

No entanto, Dewar (2014) ressalta que ainda existem preocupações em relação à Defesa Cibernética Ativa. Isso ocorre justamente porque, uma vez

[25] [Tradução própria]. No original, lê-se: *a method of achieving cyber security predicated upon the deployment of measures to detect, analyse, identify and mitigate threats to and from cyberspace in real-time, combined with the capability and resources to take proactive or aggressive action against threat agents in those agents' home networks.*

que atores estatais respondam a agressões cibernéticas com força militar convencional, podem estar ferindo normas do direito internacional. Todavia, mesmo que estivessem violando normas do direito internacional, ainda não existem legislações amplamente aceitas no Sistema Internacional sobre o que pode ou não ser realizado por Estados que foram atacados no ciberespaço, o que dificultaria qualquer tipo de retaliação e/ou sanção ao Estado que utilizasse vias tradicionais de contra-ataque.

Como citado anteriormente, não existem normas consensuais no Sistema Internacional sobre como se pode ou não responder às ofensas realizadas no ciberespaço. Portanto, há uma névoa sobre quais podem ser as consequências de tais ações. Sexton (2016) discorre sobre o uso planejado da Defesa Cibernética Ativa por parte do Reino Unido. O autor levanta o questionamento sobre se os "ataques cibernéticos", como descritos no discurso do Reino Unido, representam uso proibido da força, de forma a potencialmente chegar ao nível de ataques armados sob o direito internacional. Sexton (2016) salienta, contudo, que não existe consenso sobre o tipo de resposta que deve ser permitido no caso de ataques cibernéticos.

Os Estados Unidos discorrem sobre a questão da resiliência, quando destacam a "restauração do sistema para uma configuração segura". A resiliência é um ponto importante porque, no ciberespaço, é basicamente impossível que um Estado consiga se defender de todos os ataques que irá receber. Portanto, os Estados precisam possuir os meios necessários para restabelecer seus sistemas e voltar a funcionalidade o mais rápido possível quando sofrerem ataques de grande impacto.

O Guia de Defesa Cibernética na América do Sul (2017), de Guedes et al., traz um glossário com conceitos relevantes para a temática cibernética. A Defesa Cibernética é definida, então, como o "ato de defender o sistema crítico das Tecnologias da informação e comunicação (TICs) de um Estado" (GUEDES et al., 2017, p. 14). Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país. A definição não especifica quais ações podem ser utilizadas para defender o sistema crítico das TICs, o que abre margem para a utilização de ações ofensivas, caso o Estado seja atacado.

Conforme Galinec, Možnik e Guberina (2017, p. 273), a Defesa Cibernética se concentra em "detectar e fornecer respostas oportunas a ataques ou ameaças para que nenhuma infraestrutura ou informação seja adulterada", definição que conversa diretamente com o que é estabelecido por Estados Unidos em seus documentos oficiais de Defesa. Galinec, Možnik e Guberina (2017) argumentam que, com o aumento significativo do número de ataques cibernéticos nas últimas décadas (bem como o aumento da complexidade desses ataques), a Defesa Cibernética tem cada vez mais se tornado um aparato essencial para garantir a manutenção da segurança de entidades estatais e de informações críticas.

Rantapelkonen e Salminen (2013) discutem questões de Defesa Cibernética especificamente no âmbito de Estados nórdicos, como Suécia e Noruega. Todavia, a discussão feita pelos autores traz um panorama relevante para esta pesquisa. De acordo com eles, a Defesa Cibernética não envolve apenas a tecnologia. Também estão presentes questões como ética, normas e diferentes formas de lidar com a Segurança Cibernética. Além disso, é exposto que a cooperação entre pessoas, instituições, Forças Armadas, Estados e Organizações Internacionais precisa ser acordada (RANTAPELKONEN; SALMINEN, 2013).

Aspectos como ética, normas e diferentes formas de lidar com Segurança e Defesa Cibernética são, de fato, fatores determinísticos para a área. Como discutido anteriormente com base em Ventre (2012) e Skinner (2013), o componente humano no ciberespaço precisa sempre ser levado em consideração. Isso deve acontecer porque, como tratado por Skinner (2013), são os controladores cibernéticos (o componente humano) quem, em última instância, irão tomar as decisões de Segurança e Defesa Cibernética no ciberespaço, o que dialoga diretamente com as questões que envolvem ética e normas discutidas por Rantapelkonen e Salminen (2013).

Como apresentado anteriormente, Libicki (2009) salienta que a Defesa Cibernética compreende tudo aquilo que for necessário para fazer com que um atacante não tenha obtenha sucesso em seus esforços, e isso está presente nas definições de Estados Unidos e Reino Unido apresentadas. A definição de Souza e Almeida (2016) de que a Defesa Cibernética é compreendida por ações operacionais, de caráter ofensivo, caracterizadas por ataques

cibernéticos também se aproxima bastante das definições divulgadas por Estados Unidos e Reino Unido. Já Dewar (2014), em sua definição de Defesa Cibernética Ativa, dá ênfase a palavras como detectar e mitigar, assim como é exposto pelos Estados Unidos.

A Defesa Cibernética, portanto, pode ser compreendida como o conjunto de ações ofensivas, defensivas e exploratórias realizadas por Estados no ciberespaço com o objetivo de proteger seus sistemas de informação, suas infraestruturas críticas e, em um sentido mais amplo, a própria soberania do Estado. As ações de Defesa Cibernética visam, dessa forma, proteger o Estado de quaisquer ameaças ou possibilidades de ameaça e incluem a detecção, caracterização, combate e mitigação dessas ameaças, além da capacidade de restauração daquilo que for danificado o mais breve possível.

Em um contexto mais geral, especialmente a partir das definições de países como Estados Unidos e Reino Unido, pode-se pensar a Segurança Cibernética em um sentido mais amplo do que a Defesa Cibernética, inclusive havendo a possibilidade de, nesse caso, a Defesa estar sob o guarda-chuva da Segurança. Isso porque, diferentemente da Segurança Cibernética, a Defesa Cibernética possui objetivos mais específicos, como a realização de ações ofensivas, defensivas e exploratórias, como por exemplo as ações destacadas por Estados Unidos e Reino Unido para mitigar ataques e derrotar ameaças no ciberespaço.

É importante ressaltar que, mesmo que na prática ações de Segurança Cibernética e Defesa Cibernética acabem se encontrando e às vezes até mesmo se perpassando, é importante separá-las conceitualmente. Essa separação entre os termos é crucial para que fique claro quem são os atores responsáveis por cada ação e para a formulação de políticas públicas (GONZALES; PORTELA, 2018), bem como para que, em casos de transgressões cibernéticas, um hacker que rouba dados de cartões de crédito não seja responsabilizado da mesma forma que um Estado que ataca infraestruturas críticas de outro Estado, por exemplo.

Logicamente, ambas ações citadas acima são consideradas erradas e possuem impactos negativos para com a sociedade ou com o Estado. Todavia, os impactos causados são totalmente distintos e, por isso, devem ser julgados de acordo. Uma governança securitária estatal robusta se mostra

extremamente necessária nesse sentido, tendo em vista que, se houver diálogo e coordenação entre os organismos de Segurança Cibernética e Defesa Cibernética, eles poderão comunicar e encaminhar os casos com os quais se deparam àqueles que são responsáveis por lidar com questões X ou Y.

Sobre capacidades de Defesa Cibernética e Segurança Cibernética robustas, sem dúvida são desejáveis e até necessárias para garantir melhor funcionamento do aparato estatal e para proteger sua soberania, território, população e interesses. Todavia, cada vez mais tem sido levantado o debate acerca da atuação do Estado no ciberespaço versus liberdades de indivíduos. É importante destacar que não se propõe aqui discutir sobre ações boas ou ruins de indivíduos no ciberespaço, mas sim refletir sobre um possível poder exacerbado do Estado nesse domínio que acabe por reprimir ou até mesmo penalizar cidadãos sob a ótica da Defesa Cibernética, que é a mesma que dita as regras para lidar com ataques advindos de outras nações ou grupos terroristas, por exemplo.

Conforme Dipert (2010), apesar de haver tentativas por parte de Estados e organismos internacionais, como a OTAN, ainda não se tem resoluções e/ou acordos internacionais amplamente aceitos para lidar com as questões que surgem no ciberespaço. Segundo Ayres Pinto e Grassi (2020), essa lacuna existente na legislação internacional pode ser intencional, uma vez que, quanto menos restrita for a legislação, mais os Estados poderão agir da forma que melhor atenda a seus interesses sem correr o risco de grandes represálias. O que, de fato, faz sentido. Estados com grande poderio cibernético como China, Estados Unidos, Reino Unido, Rússia, entre outros, não precisam querer restringir e/ou afunilar quais ações de Defesa Cibernética podem ou não ser utilizadas em um regime internacional, porque se isso de fato vir a ocorrer a nível global, esses Estados estariam reprimindo um poder que eles possuem e podem utilizar da forma que melhor sirva a seus objetivos e que outros Estados ainda não conseguiram alcançar.

Posto isso, verifica-se que é plausível fazer uma separação entre Segurança Cibernética e Defesa Cibernética e que, inclusive, essa separação tende a ser benéfica tanto para os atores estatais que atuam nessas esferas, como para a sociedade em geral, de forma a evitar que o Estado possa acabar agindo de forma controladora até mesmo sobre sua própria população. A

Segurança Cibernética em um sentido mais amplo, portanto, representaria a capacidade de proteger os sistemas conectados à internet e as informações que estão contidas nesses sistemas, bem como a capacidade de garantir a segurança da população (representada pela sociedade da informação no espaço cibernético). E a Defesa Cibernética, de forma mais específica, representaria as ações ofensivas, defensivas e exploratórias realizadas pelos Estados no ciberespaço com o intuito de proteger seja seus sistemas, dados, infraestruturas, seja a sua própria população e soberania.

4 GOVERNANÇA SECURITÁRIA ESTATAL DE ESTADOS UNIDOS E REINO UNIDO

O espaço cibernético representa desafios para a governança global. Conforme Emerson (2016) e Liaropoulos (2016), esses desafios surgem devido a assimetria, anonimidade e recursos de uso dual (que são utilizados tanto por civis como pelas Forças Armadas) presentes no domínio e que desafiam os conhecimentos tradicionais de segurança, fronteiras, privacidade, direitos humanos e soberania, por exemplo (LIAROPOULOS, 2017). Todas essas questões são complexas, únicas e possuidoras de peculiaridades próprias. Portanto, é de se esperar que enfrentar todas elas em uma única esfera - no caso, o ciberespaço - seja uma tarefa árdua. Nesse sentido, torna-se necessário um olhar cuidadoso e atento do Estado para a alocação de atores responsáveis por lidar com cada uma dessas questões.

Dessa forma, após explorar os conceitos de governança, governança securitária, ciberespaço, defesa cibernética e segurança cibernética, ao longo deste capítulo - com o arcabouço adquirido durante os primeiros dois capítulos da presente dissertação - serão analisadas as estruturas de governança securitária estatal de Estados Unidos e Reino Unido voltadas para lidar com os riscos e ameaças presentes no domínio cibernético. Destaca-se, novamente, que devido ao tempo disponível para a realização da pesquisa, serão considerados apenas atores estatais de Segurança e Defesa na análise das estruturas de governança securitária de ambos os países.

4.1 OS ESTADOS UNIDOS E SEUS ORGANISMOS DE SEGURANÇA E DEFESA CIBERNÉTICA

4.1.1 Desenvolvimento da ARPANET nos Estados Unidos

Antes de adentrar a temática dos organismos securitários estadunidenses, é importante destacar a importância desse país na criação da internet e do ciberespaço. Durante a Guerra Fria - e em resposta ao lançamento do *Sputnik*[26] pela União Soviética -, foi criada a *Advanced Research Projects Agency* (ARPA), direcionada não apenas a objetivos

[26] Primeiro satélite artificial colocado em órbita ao redor da Terra em 1957.

militares, mas também à pesquisas (HAUBEN, 2007). A ARPANET, por sua vez, representava um dos muitos programas existentes na ARPA, encabeçado pelo *Information Processing Techniques Office* (IPTO). O objetivo desse departamento, conforme Castells (2003), consistia em estimular o desenvolvimento da computação interativa. Nesse sentido, a ARPANET representava uma forma de possibilitar diversos centros e grupos de pesquisa que faziam parte da ARPA a compartilhar informações em tempo real (CASTELLS, 2003).

Para tornar possível uma interação com redes de computadores externas a ARPA, o *Information Processing Techniques Office* passou a utilizar a tecnologia de transmissão de telecomunicações por pacote desenvolvida por Baran na *Rand Corporation* e Davis no *British National Physical Laboratory* (CASTELLS, 2003). Apesar do objetivo inicial da ARPANET não ter sido de caráter militar, foi a partir da interação do *Information Processing Techniques Office* com a *Rand Corporation* que a internet adquiriu aspecto militarizado: a *Rand* ofereceu ao Departamento de Defesa dos Estados Unidos a construção de um sistema militar de comunicações descentralizado, e que poderia ser mantido até mesmo caso houvesse um ataque nuclear (CASTELLS, 2003). É importante destacar que, apesar de haver trabalhos similares em outros países, com a criação da ARPANET em 1969, este foi considerado como o primeiro protótipo de internet do mundo (GUEDES et al., 2017).

Com o passar dos anos e com o aumento exponencial de usuários da internet e do ciberespaço, torna-se inegável a importância e necessidade desse domínio seja para indivíduos, empresas ou para Estados. Conforme o *Department of Homeland Security* (DHS) dos Estados Unidos, com o aumento da conectividade de pessoas e de aparelhos à internet, há o surgimento de um campo passível de ataques que adentra o país por meio de qualquer casa estadunidense com acesso à internet. Nesse sentido, o DHS considera o ciberespaço como o domínio atual mais dinâmico e de maior ameaça ao país (UNITED STATES, 2019).

Tendo em vista que, no começo, a ARPANET tinha como objetivo a comunicação em tempo real de diversos servidores, pode-se inferir que o primeiro protótipo reconhecido de internet não possuía apenas objetivos militares. Entretanto, ao introduzir esse projeto ao Departamento de Defesa

estadunidense e, a partir disso, tê-lo ampliado para um sistema de comunicação a ser utilizado pelas Forças Armadas para garantir uma comunicação ininterrupta, o projeto adquiriu caráter militarizado. Além disso, ressalta-se que apesar de ter sido ampliada por meio de objetivos militares, com a popularização da internet e com o crescente aumento de usuários, ela deixou de ser um ambiente "seguro" para a comunicação militar estadunidense e passou a possuir diversas outras facetas para além daquilo que havia sido pensado para seu funcionamento.

É importante ressaltar que ciberespaço vai muito além da Internet ou da ARPANET quando ela foi criada: além da parte virtual, fazem parte do domínio cibernético componentes físicos como cabos submarinos, satélites e até mesmo os seres humanos que constroem, navegam e tomam decisões que afetam o ciberespaço. Conforme Ayres Pinto (2017), o primeiro exemplo de utilização do ciberespaço ocorreu com a criação do telégrafo, uma vez que esse objeto envia informações via fios. Contudo, é inegável que houve uma expansão significativa do ciberespaço (e do seu uso) a partir da criação da Internet e da sua utilização pelas diversas camadas da sociedade.

Já os nós de rede, que são explorados a seguir, representam as partes físicas que constituem uma rede. Usualmente, os nós incluem qualquer dispositivo que recebe e envia informações. Todavia, os nós também podem receber e armazenar dados, retransmitir informações para outro lugar ou criar e enviar dados (FISHER, 2021). Abaixo será exposta tabela desenvolvida com base em Lukasic (2011) que demonstra o aumento de nós da ARPANET ao longo dos anos de acordo com instituições investidoras:

Tabela 1: Aumento de nós iniciais da ARPANET por instituições investidoras

Data	IPT (R&D)	ARPA (R&D) (Non-IPT)	Military (R&D)	Non-DOD (R&D)	Total
Janeiro 1970	4	0	0	0	4
Junho 1970	9	0	0	0	9
Dezembro 1970	13	0	0	0	13
Setembro 1971	15	0	1	1	17
Março 1972	17	0	6	2	25

Agosto 1972	17	2	7	3	29
Setembro 1973	20	3	11	9	43
Junho 1974	21	3	14	9	47
Julho 1975	24	3	18	10	55
Julho 1976	24	3	21	10	58
Julho 1977	24	3	24	10	61

Fonte: elaboração própria com base em Lukasic (2011).

Como identificado por Lukasic (2011), é possível identificar três tendências nos nós de rede da ARPANET. Em primeiro lugar, tem-se o investimento contínuo de pesquisa e desenvolvimento do *Information Processing Techniques Program* (IPT) ao longo dos anos. A segunda tendência identificada ocorre por meio de pesquisa e desenvolvimento militar, impulsionada pela criação de sites e nós militares, incluindo um nó da *National Aeronautics and Space Administration* (NASA). A terceira e última tendência diz respeito à saturação no aumento geral de nós, o que ocorre ao mesmo tempo em que há crescimento de tráfego e número de usuários (LUKASIC, 2011).

De acordo com a tabela, fica claro que existe um investimento contínuo do *Information Processing Techniques Program* (IPT na tabela) em pesquisa e desenvolvimento da ARPANET. Contudo, outro ponto que chama atenção na tabela, é a existência de nós adquiridos por meio de investimento militar e a rapidez em que ocorre seu aumento. É possível verificar que via investimento militar se passa de 0 nós em 1970 para onze 11 no ano de 1973 e 24 nós em 1977, atingindo, então, o mesmo número de nós que o *Information Processing Techniques Program* em um período de tempo significativamente menor.

A virada nos nós adquiridos se torna perceptível em março de 1972, quando há um aumento de 2 nós obtidos por meio do IPT e um aumento de 5 nós adquiridos por meio de investimento militar. Essa virada significa que, naquele momento, o número de novos nós para fins internos da ARPA foi menor do que o de nós criados para instalações e missões militares (LUKASIC, 2011). É um dado relevante porque demonstra que, a partir do momento em que foi percebido pelo Departamento de Defesa dos Estados Unidos que o protótipo de Internet poderia ser utilizado para fins militares e de Defesa, houve interesse e investimento.

4.1.2 Principais organismos da governança securitária do ciberespaço estadunidense

Os Estados Unidos possuem inúmeros departamentos, escritórios e agências envolvidos com questões relacionadas à defesa ou segurança cibernética - além de organismos que não são voltados exclusivamente para lidar com questões cibernéticas, mas que também atuam nessa frente, como é o caso do *Federal Bureau of Investigation* (FBI). Todavia, é importante se ter em mente que, no presente estudo de caso, não serão explorados todos os organismos estadunidenses vinculados a ações de defesa e segurança cibernética, posto que essa lista não é exaustiva.

Quadro 6 - órgãos e funções na governança securitária do ciberespaço dos Estados Unidos

Órgão	Função
Department of Homeland Security (DHS)	O DHS constrói as capacidades nacionais para se defender de ataques cibernéticos.
Cybersecurity and Infrastructure Security Agency (CISA)	A CISA lidera o esforço nacional para entender, gerenciar e reduzir o risco para a infraestrutura física e cibernética estadunidense.
United States Cyber Command (USCYBERCOM)	O Comando tem três áreas de foco principais: defender a rede de informações do Departamento de Defesa, fornecer suporte aos comandantes combatentes para a execução de suas missões ao redor do mundo e fortalecer a capacidade dos Estados Unidos de resistir e responder a ataques cibernéticos.
National Security Agency (NSA)	A NSA fornece alertas de segurança cibernética e orientações técnicas, além de avaliações de ameaças.
Federal Bureau of Investigation (FBI)	O FBI age como investigador de ataques cibernéticos orquestrados por criminosos, adversários e terroristas.
U.S. Secret Service	O Serviço Secreto investiga crimes financeiros no ciberespaço.
Department of Justice's Cybersecurity Unit	A Unidade de Segurança Cibernética do Departamento de Justiça ajuda a moldar a legislação de segurança cibernética para proteger as redes de computadores dos Estados Unidos e as vítimas individuais de ataques cibernéticos.
Department of Defense (DOD) Cyber Command	O Comando Cibernético do DOD coordena o planejamento e as operações do ciberespaço para defender e promover os interesses nacionais, enquanto o *DOD Cyber Crime Center* fornece serviços forenses digitais, treinamento e análise cibernética.

Fonte: elaboração própria com base em Hegen (2020).

4.1.2.1 Funcionamento do *Department of Homeland Security* (DHS) e da *Cybersecurity and Infrastructure Security Agency* (CISA)

O *Department of Homeland Security* dos Estados Unidos possui como missão principal garantir a segurança do Estado contra as ameaças enfrentadas. Para tal, o órgão conta com um total de 240 mil funcionários em empregos nas mais diversas áreas, como aviação, segurança de fronteiras, respostas emergenciais, segurança cibernética, inspetores de instalações químicas, entre outros (ESTADOS UNIDOS, 2021). A instituição destaca cinco missões como principais para a proteção da nação:

1. ajuda em caso de desastres;
2. proteção da economia;
3. proteção de fronteiras;
4. segurança do ciberespaço e das infraestruturas críticas;
5. impedir ações terroristas e ameaças à segurança interna.

A partir da lista acima, torna-se perceptível a relevância empregada pelo DHS quanto a necessidade de haver um olhar atento à segurança do ciberespaço e das infraestruturas críticas do Estado para garantir o melhor funcionamento da sociedade e, até mesmo, para garantir a soberania dos Estados Unidos. Como supracitado, o organismo destaca a ajuda em caso de desastres, a proteção da economia, a proteção de fronteiras e o impedimento de ações terroristas em território nacional. Especificamente sobre a segurança do ciberespaço e das infraestruturas críticas, é destacado a atuação da CISA - que é a *Cybersecurity and Infrastructure Security Agency* - organismo subordinado ao DHS e que é responsável por proteger os Estados Unidos contra ataques cibernéticos, bem como responsável por proteger as infraestruturas críticas do país. A atuação da *Cybersecurity and Infrastructure Security Agency* será explorada a seguir.

De acordo com o governo estadunidense (2021), o *Department of Homeland Security* (DHS) é responsável por alguns pontos específicos vinculados ao ciberespaço. Entre as responsabilidades do DHS vinculadas ao ciberespaço estão: 1. prover assistência à entidades potencialmente impactadas por ataques cibernéticos; 2. analisar o potencial impacto de

ataques em infraestruturas críticas (IFCs); 3. investigar os responsáveis em conjunto com autoridades policiais e 4. coordenar a resposta nacional à acidentes cibernéticos significativos. As responsabilidades apresentadas pelo DHS remetem ao caráter de "segurança pública" da segurança cibernética desenvolvido por Von Solms e Van Niekerk (2013), o qual aponta a proteção de usuários no ciberespaço seja em capacidade pessoal, social ou nacional.

Tanto o *Department of Homeland Security* como a *Cybersecurity and Infrastructure Security Agency* representam organismos de Segurança, como os próprios nomes dizem. Todavia, a ação de ambos organismos vai além da definição de Segurança dos Estados Unidos (2021), a qual, de fato, prevê medidas para proteger instalações militares, mas não prevê ações ofensivas. A definição de Segurança Cibernética dos Estados Unidos, por sua vez, é referente a atividade, processo, habilidade ou capacidade de proteger dados e informações contra danos, uso não autorizado, modificação ou exploração (ESTADOS UNIDOS, 2021) e não discorre, em nenhum momento, sobre funções ofensivas e/ou de contra-ataque, assim como as definições de Segurança Cibernética de autores como Lewis (2006); Cavelty (2010); Souza (2013) e Pelton e Singh (2015) também não apontam tais atribuições.

A atuação do DHS e da CISA, portanto, vai além do espectro das definições de Segurança e Segurança Cibernética, uma vez que a CISA é responsável não apenas por promover assistência, analisar impactos e identificar responsáveis por ataques cibernéticos, como também é responsável por coordenar a resposta nacional à ataques cibernéticos, ataques que podem inclusive ter sido, inclusive, realizados por atores externos e/ou outros Estados, o que os colocaria, em teoria, a cargo de organismos de Defesa Cibernética.

No começo, o *Department of Homeland Security* possuía diversas divisões cibernéticas, cada uma encarregada de diferentes objetivos. Todavia, em 2018, o então presidente dos Estados Unidos, Donald Trump, assinou uma lei que reorganizou a estrutura cibernética do DHS a transformando, então, na *Cybersecurity and Infrastructure Security Agency* (CISA). Conforme Hofmanova (2019), ao introduzir a CISA foi demonstrado a importância das áreas envolvidas, bem como foi apontada a necessidade de aprimorar a proteção do ciberespaço e das infraestruturas críticas estadunidenses.

O propósito da *Cybersecurity and Infrastructure Agency* é, de acordo com o governo estadunidense, o de mobilizar uma defesa coletiva das infraestruturas críticas do país. Além disso, a CISA possui como atribuição responsabilidades como a liderança nos esforços da gestão de risco da nação, o que significa que é este o órgão que irá reunir as diversas partes interessadas em identificar riscos de maneira colaborativa e priorizá-los conforme os riscos apresentados, desenvolver soluções e, por fim, colocar em prática o que foi estabelecido pelas partes envolvidas para que seja possível, então, garantir a estabilidade das funções críticas do Estado (ESTADOS UNIDOS, 2021). Nesse sentido, fica claro o caráter de liderança da CISA, tendo em vista que o órgão realiza ações ofensivas contra as ameaças cibernéticas identificadas às infraestruturas críticas (DEWAR, 2014; GUEDES et. al, 2017; GALINEC et. al, 2017; ESTADOS UNIDOS, 2021). O que reforça, mais uma vez, o transbordamento da atuação de um organismo de Segurança, que não somente é responsável por lidar com atribuições teoricamente de Defesa, bem como possui caráter de liderança nessa frente.

No início de 2021, o *Department of Homeland Security* publicou uma visão geral do orçamento da *Cybersecurity and Infrastructure Security Agency* para o ano fiscal de 2021. Portanto, a seguir será organizado um quadro discriminando quais foram os gastos elencados pelos Estados Unidos, com o intuito de compreender quais são as prioridades do país no que diz respeito a sua segurança cibernética, bem como à segurança de suas infraestruturas críticas. Para justificar o orçamento referente à segurança cibernética, o DHS enfatiza que em um mundo globalmente interconectado, as infraestruturas críticas estadunidenses (bem como o *American way of life*) enfrentam uma gama de ameaças que representam grandes riscos para o país e para sua população.

Quadro 7 - investimento estadunidense à CISA para segurança cibernética e segurança de infraestruturas críticas no ano de 2021

Investimento em dólares	**Discriminação do investimento**
1.1 bilhão	para esforços de segurança cibernética para proteger o domínio federal ".gov", inclusive de redes civis, e para fazer parceria com o setor privado para aumentar a segurança de redes críticas;

96.1 milhões	para esforços de segurança de infraestrutura para proteger e aumentar a resiliência das infraestruturas críticas contra os perigos existentes por meio do gerenciamento de riscos e colaboração com a comunidade de infraestrutura crítica;
157.6 milhões	para garantir a interoperabilidade da comunicação de emergência e fornecer assistência e apoio às partes interessadas federais, estaduais, locais e territoriais;
166.7 milhões	para operações integradas da linha de frente da CISA, atividades externas para garantir suporte contínuo e resposta rápida às necessidades críticas;
91.5 milhões	para que o *National Risk Management Center* forneça análise de consequências de infraestrutura, suporte a decisões e recursos de modelagem para parceiros dos setores público e privado;
37.5 milhões	para o engajamento das partes interessadas e requisitos para promover a colaboração, coordenação e uma cultura de responsabilidade compartilhada para gerenciamento de risco de infraestruturas críticas nacionais e resiliência com parceiros do setor federal, estadual, local, tribal, territorial e privado nos Estados Unidos, bem como com parceiros internacionais no exterior;
141.1 milhões	para atividades de apoio à missão.

Fonte: elaboração própria com base em Estados Unidos (2021).

Por meio da visualização e leitura do quadro acima, é possível perceber que, apesar de haver sete discriminações para os investimentos em segurança cibernética e segurança das infraestruturas críticas dos Estados Unidos, o dinheiro não foi alocado igualmente entre as partes, o que sugere que exista certa hierarquia entre as demandas a serem atendidas pela CISA. Entre as sete áreas que receberam investimento em 2021, todavia, é perceptível que houve uma área com investimento muito maior do que as outras.

Os esforços de segurança cibernética para proteger o domínio federal ".gov" obtiveram um investimento de 1.1 bilhão de dólares em 2021, número que corresponde a um valor 6.59 vezes maior do que o valor destinado às operações integradas da linha de frente da CISA, atividades externas para garantir suporte contínuo e resposta rápida às necessidades críticas (166.7 milhões), segunda área de maior investimento. Com isso em vista, percebe-se que o governo estadunidense é bastante dependente de sistemas de tecnologia da informação e redes de computadores para realizar atividades e operações essenciais, como a comunicação, o fornecimento de energia e água, sistemas financeiros, entre outros.

É importante ressaltar que, não é porque uma entre as sete áreas obteve um investimento díspar, que as outras áreas não são importantes. O

mais provável é que, para o governo dos Estados Unidos, a garantia de proteção do domínio .gov seja urgente, devido a enorme quantidade de atores capazes de ameaçar os sistemas de informação, as redes de computadores, e tudo aquilo que estiver vinculado a eles (ESTADOS UNIDOS, 2021). A lista de possíveis atores que representam ameaças aos Estados Unidos (e a outros Estados) varia de hackers não sofisticados a atores estatais, e os ataques podem possuir como objetivo o roubo de informações, interromper ou negar acesso a serviços ou, até mesmo, destruir sistemas críticos de informação.

Tendo em vista as outras áreas de investimento, também se pode inferir a importância atribuída pelos Estados Unidos para outras ações. Como, por exemplo, esforços para segurança de infraestruturas; garantia de interoperabilidade da comunicação de emergência e fornecimento de assistência e apoio a órgãos federais, estaduais, locais e territoriais; fornecimento de análise de consequência de infraestruturas (em parceria com os setores público e privado), entre outros. Essas ações, quando realizadas, servem para garantir maior segurança e resiliência para as infraestruturas críticas do país.

4.1.2.2 Atividades do *Federal Bureau of Investigation* (FBI) e do *Department of Justice's Cybersecurity Unit* voltadas para o ciberespaço

O FBI é uma organização de segurança nacional voltada para questões de inteligência - com foco em ameaças - e com responsabilidades de inteligência e de aplicação da lei. Esse órgão é o principal braço investigativo do Departamento de Justiça dos Estados Unidos e, por isso, além de investigar os crimes especificamente atribuídos a ele, também fornece serviços a outras agências. Além disso, o FBI coleta, compartilha e analisa inteligência tanto para apoiar as investigações encabeçadas por ele, como para apoiar investigações desenvolvidas por parceiros, de forma a visualizar o melhor cenário e conseguir combater as ameaças existentes à segurança do país (ESTADOS UNIDOS, 2021).

A estratégica cibernética do FBI pressupõe que o órgão será capaz de impor riscos e consequências aos seus adversários no ciberespaço. Nesse sentido, o objetivo apontado pelo FBI é o de alterar o comportamento de atores

criminosos não-estatais, bem como de atores estatais, que tentem comprometer redes de computador estadunidenses, roubar propriedade intelectual ou finanças, ou que almejem colocar as infraestruturas críticas do país em risco. O FBI ainda salienta que, para conseguir atingir seus objetivos, utiliza uma gama de autoridades mista, capacidades e parcerias. O discurso empregado pelo FBI remete ao conceito de poder apresentado por Morgenthau (2003). Para Morgenthau, poder constitui a capacidade de fazer com que outro aja de acordo com os seus interesses. A vontade (e capacidade) de fazer com que o outro aja de acordo com aquilo que você quer está presente no discurso do FBI no momento em que o órgão coloca como objetivo alterar o comportamento de atores estatais e não-estatais que representem ameaça para os Estados Unidos.

Outro ponto central para o organismo é a atividade de inteligência. São coletadas e compartilhadas informações ao mesmo tempo em que o órgão se comunica com as "vítimas", ou seja, aqueles que são almejados via crimes cibernéticos. Para que seja possível interceptar a ação de atores adversários, o FBI trabalha com outros organismos federais, parceiros estrangeiros e com o setor privado. São essas parcerias que permitem que o órgão realize a defesa de redes de computador e sistemas de informação, atribua atividades maliciosas aos atores responsáveis, sugira sanções e revide possíveis agressões (ESTADOS UNIDOS, 2021). O FBI, apesar de atuar como organismo de polícia de investigação e serviço de inteligência interno (ambas responsabilidades domésticas), possui entre suas atribuições a capacidade de revidar agressões. Mais uma vez, assim como ocorre no caso do DHS e da CISA, tem-se um organismo sob jurisdição de atuação interna a cargo de responsabilidades tipicamente de Defesa Cibernética. Ressalta-se, portanto, que a atuação do FBI excede a alçada do que está previsto nas definições de Segurança e Segurança Cibernética do País (ESTADOS UNIDOS 2020; ESTADOS UNIDOS 2021).

A atuação em equipe, que é constantemente enfatizada pelo FBI em documentos e *websites*, é frequente. A *National Cyber Investigative Joint Task Force* (NCIJTF), que é encabeçada pelo FBI e trabalha em conjunto com organismos como a *Central Intelligence Agency*, *Department of Defense*, *Department of Homeland Security*, *National Security Agency*, entre outros, é a

força tarefa que serve como o centro cibernético cuja responsabilidade principal é coordenar, integrar e compartilhar informações que sirvam para apoiar as investigações de ameaças cibernéticas. Além disso, a NCIJTF também possui em seu rol de deveres fornecer e apoiar análises de inteligência para tomadores de decisão e empreender esforços contínuos para lidar com as ameaças cibernéticas que os Estados Unidos enfrentam (ESTADOS UNIDOS, 2021). Essa ação conjunta encabeçada pelo FBI vai de encontro à definição de governança securitária de Krahmann (2003), a qual prevê a atuação conjunta de atores para que se torne possível coordenar necessidades e interesses.

Sobre a forma como o FBI trabalha (especialmente com relação à ações/operações/times cibernéticos), o órgão destaca cinco frentes: 1. presença de esquadrões cibernéticos treinados em todos os cinquenta e seis escritórios, trabalhando junto aos parceiros de cada força tarefa; 2. o *Cyber Action Team*, que pode ser introduzido em qualquer lugar no país em questão de horas para responder à incidentes de grande escala; 3. presença de assistentes cibernéticos trabalhando como adidos em embaixadas ao redor do globo; 4. o *Internet Crime Complaint Center* (IC3), que coleta relatórios de crimes contra o público na internet e, por fim, 5. o *CyWatch*, que é o centro de operações do FBI que funciona 24 horas por semana e fornece suporte contínuo para rastrear incidentes e comunicar os escritórios ao redor do país (ESTADOS UNIDOS (2021).

As cinco frentes apresentadas pelo FBI demonstram a importância atribuída ao setor cibernético pelo órgão e salientam a necessidade de haver coordenação para lidar com ameaças e adversidades que possam surgir no ciberespaço. Os esquadrões cibernéticos, o *Cyber Action Team* e os assistentes cibernéticos atuando como adidos em embaixadas podem ser relacionados com os chamados "controladores" de Skinner (2013). Os controladores, para o autor, representam o efetivo alocado para lidar com a defesa do domínio cibernético e, para além disso, podem ser considerados como parte integrante do componente humano do ciberespaço, visto que são esses atores que irão tomar decisões de Segurança e Defesa Cibernética (VENTRE, 2012; SKINNER, 2013).

Por sua vez, a Unidade de Cibersegurança do Departamento de Justiça dos Estados Unidos foi criada em dezembro de 2012, dentro da seção de

crimes de computador e propriedade intelectual. O objetivo da unidade consiste em atuar como um ponto central para aconselhamento especializado, bem como para orientação legal sobre como "a vigilância eletrônica e os estatutos de fraude e abuso de computador impactam a segurança cibernética" (ESTADOS UNIDOS, 2021, n/p). Entre seus objetivos estão a garantia de que as autoridades policiais sejam utilizadas de maneira eficaz ao levar criminosos à justiça ao mesmo tempo em que seja protegida a privacidade dos estadunidenses.

Além disso, a unidade também atua de forma a moldar a legislação referente à segurança cibernética para proteger a soberania dos Estados Unidos, suas infraestruturas críticas e a sua população (ESTADOS UNIDOS, 2021). A Unidade de Cibersegurança, diferentemente do que foi visto nos casos do DHS, CISA e FBI, elenca apenas atividades de segurança cibernética que vão de encontro as definições de Segurança e Segurança Cibernética do País (ESTADOS UNIDOS, 2020; ESTADOS UNIDOS, 2021). Isso porque, apesar de discorrer sobre a proteção da população e de infraestruturas críticas, não são apontadas ações ofensivas ou medidas de contra-ataque em seu rol de atividades, por exemplo. Por fim, é destacado pelo Departamento de Justiça o envolvimento da unidade com o setor privado, de maneira a promover práticas legais seguras nesse ambiente. O que é interessante porque, assim como órgãos estatais de Segurança e Defesa Cibernética, o setor privado também possui papel relevante na administração do ciberespaço (KLIMBURG; FAESEN, 2018).

4.1.2.3 *US. Secret Service* e a proteção da infraestrutura do sistema financeiro estadunidense

O Serviço Secreto dos Estados Unidos foi criado em 1865, para que fosse combatido o aumento da moeda falsificada após a Guerra Civil. Contudo, ao passo que o sistema financeiro foi evoluindo, as responsabilidades do Serviço Secreto também foram alteradas. Atualmente, os agentes do Serviço Secreto estadunidense estão espalhados ao redor do mundo, em escritórios, lidando com os diversos crimes financeiros que ocorrem no século XXI, e em

especial aqueles realizados por intermédio do espaço cibernético (ESTADOS UNIDOS, 2021).

O objetivo do serviço secreto estadunidense, no que diz respeito à atuação vinculado ao ciberespaço, é o de proteger a infraestrutura financeira dos Estados Unidos e manter um ambiente seguro para a população conduzir suas transações financeiras, bem como investigar crimes cibernéticos com objetivos financeiros. O ponto central desse organismo está, assim como no caso do FBI, em uma força tarefa conjunta. Nesse caso, representada pela *Cyber Fraud Task Forces* (CFTFs), que trabalha junto a outras agências de investigação, promotores, indústria privada e academia (ESTADOS UNIDOS, 2021).

A *Cyber Fraud Task* lida com crimes cibernéticos por meio de prevenção, detenção, mitigação e investigação. Os objetivos dessa força-tarefa, ou seja, a prevenção, detenção, mitigação e investigação de crimes cibernéticos, se relacionam diretamente com a definição de Defesa Cibernética dos Estados Unidos (2021), a qual inclui ações para detectar caracterizar, combater e mitigar ameaças e atividades não autorizadas, bem como com a definição de Defesa Cibernética Ativa de Dewar (2014), que discorre sobre medidas para detectar, analisar, identificar e mitigar ameaças no ciberespaço. O Serviço Secreto dos Estados Unidos, todavia, está sob o guarda-chuva do *Department of Homeland Security*, assim como a CISA. Portanto, mais uma vez, tem-se um organismo de segurança com atribuições de defesa cibernética.

O Serviço Secreto lista alguns dos principais tipos de serviço realizados pelos seus funcionários, como os respondedores de intrusão, que são a linha de frente do Serviço Secreto para combater ataques de *malware* e intrusões de rede em grandes escalas e, assim como no caso dos funcionários do FBI, se assemelham aos controladores de Skinner (2013). Já os investigadores, analistas e examinadores forenses são aqueles que contribuem com a apreensão de criminosos cibernéticos transnacionais envolvidos em violações de dados em grande escala, lidar com serviços de hospedagem vinculados a atividades criminosas e com o tráfico de dados financeiros roubados, bem como outros crimes cibernéticos (ESTADOS UNIDOS, 2021).

4.1.2.4 A Dualidade do Departamento de Defesa dos Estados Unidos no Ciberespaço: *United States Cyber Command* e *National Security Agency*

Antes de discutir as missões de cada um dos dois organismos vinculados ao Departamento de Defesa dos Estados, é importante se ter em mente que, diferentemente dos organismos apresentados até aqui, tanto o USCYBERCOM como a NSA são comandados pela mesma pessoa. Desde maio de 2018, os cargos são assumidos pelo General Paul Nakasone, Comandante do *U.S. Cyber Command* (USCYBERCOM) e Diretor da *National Security Agency* (NSA) (ESTADOS UNIDO, 2021). Além de estarem sob o mesmo comando, os organismos funcionam de maneira próxima e por isso são analisados em conjunto.

O Comando Cibernético dos Estados Unidos (*U.S. Cyber Command*) faz parte das Forças Armadas do país e é encarregado de monitorar e administrar operações no ciberespaço, bem como de garantir a segurança cibernética de tecnologias da informação militares e governamentais. Entre as principais responsabilidades do USCYBERCOM estão o planejamento, coordenação, sincronização e condução de operações cibernéticas e, sobretudo, a capacidade de realizar operações cibernéticas em larga escala contra ataques cibernéticos (ESTADOS UNIDOS, 2018). Responsabilidades essas que são amparadas pela definição de Defesa Cibernética dos Estados Unidos, visto que estão previstas ações tomadas dentro do ciberespaço para derrotar as ameaças que violem ou ameacem a segurança do ciberespaço para os Estados Unidos (ESTADOS UNIDOS, 2021).

Iniciado em 2009 com o objetivo de criar um setor militar separado para focar totalmente em operações de segurança e defesa do ciberespaço, em 21 de maio de 2010 o Comando Cibernético foi fundado. A Estratégia de Defesa Nacional de 2018 dos Estados Unidos discute a forma como adversários dos Estados Unidos têm "transferido" esforços para operações no ciberespaço. Ou seja, o país admite que com o advento do espaço cibernético e com o aumento constante das ameaças existentes nele para o país e sua população, tornou-se necessário um braço militar capaz de lidar com os crescentes perigos desse domínio.

Um ponto a ser destacado sobre o Comando Cibernético dos Estados Unidos é o seu vínculo com a *National Security Agency* (NSA), desde a sua fundação em 2010. Desde a criação do USCYBERCOM, ambos os órgãos são submetidos ao mesmo Comandante. O objetivo inicial dessa ligação entre USCYBERCOM e NSA era que o Comando Cibernético pudesse se beneficiar das *expertises*, capacidades e experiências da NSA, o que de fato auxiliou o Comando Cibernético a atingir sua capacidade operacional por completo (SCHOKA, 2019). Essa relação tinha o objetivo de ser temporária, contudo, os órgãos continuam interligados.

Os Estados Unidos assumem uma postura assertiva quanto ao ciberespaço no discurso presente em seus documentos oficiais de defesa. O país intitula o USCYBERCOM como os "ciberguerreiros" que operam diariamente no espaço cibernético lidando com os inimigos da nação, inclusive outros países (ESTADOS UNIDOS, 2018). Entre os aprendizados destacados pelo país, há destaque para a necessidade de impedir ataques antes que eles penetrem a defesa cibernética ou enfraqueçam qualquer força militar. É interessante destacar o aprendizado sobre o qual os Estados Unidos falam, uma vez que é de suma importância que seja compreendido onde ocorreram falhas ou pontos cegos para evitar que esses mesmos pontos sejam explorados em futuros ataques, de forma a aumentar a resiliência cibernética do Estado.

Por meio de operações persistentes e integradas, os Estados Unidos esperam influenciar o comportamento de seus adversários e, talvez, até introduzir certo grau de incerteza, o que pode estimular os inimigos a desistirem de atacar (ESTADOS UNIDOS, 2018). O discurso dos Estados Unidos pode ser relacionado com a definição de poder de Weber (1978), a qual define o poder como a probabilidade de um ator dentro de uma relação social realizar sua própria vontade apesar da resistência do outro, que é basicamente o que os Estados Unidos esperam conseguir ao inserir incerteza na tomada de decisão de seus inimigos. Portanto, ao introduzir incerteza no cálculo de seus inimigos no ciberespaço, os Estados Unidos estão projetando o seu poder.

Todavia, o documento estadunidense não cita exemplos reais sobre a projeção de poder para que seja afirmado se a inserção de incerteza tem ou não influenciado atores inimigos a não atacarem os Estados Unidos. Ainda de

acordo com a postura assertiva estadunidense, é salientado que o propósito do Comando Cibernético é o de atingir a superioridade no ciberespaço de forma a aproveitar e manter iniciativas táticas e operacionais no domínio, obtendo, portanto, vantagens estratégicas em relação aos seus adversários (ESTADOS UNIDOS, 2018).

O Comando Cibernético dos Estados Unidos possui cinco ações imperativas em sua atuação no ciberespaço, ações essas que suportam umas às outras, fazendo com que o sucesso de uma aumente a chance de sucesso da outra. As ações discutidas a seguir, portanto, são as ações que ditam como o USCYBERCOM irá atuar no ciberespaço (ESTADOS UNIDOS, 2018).

1. Alcançar, superar e manter a superação das capacidades de seus adversários. Para alcançar tal objetivo, o Comando Cibernético destaca que é preciso antecipar e identificar mudanças tecnológicas, bem como explorar e operacionalizar as tecnologias e inovações emergentes de forma eficaz e mais rápida do que os outros;
2. Obter vantagens no ciberespaço que possibilitem o aprimoramento de operações em todos os outros domínios. O que ocorre por meio do desenvolvimento de vantagens na preparação para operações conjuntas em conflito e, também, durante conflitos;
3. Criar vantagens informacionais para apoiar resultados operacionais e alcançar impacto estratégico. Essas vantagens são criadas por meio do aprimoramento das informações entregues aos comandantes, da integração das operações no ciberespaço com as operações informacionais e da unificação de inteligência que serve como suporte às operações cibernéticas e informacionais;
4. Operacionalização do campo de batalha para manobras ágeis e responsivas. Para que essa operacionalização ocorra, é necessário que seja facilitada a velocidade e agilidade das operações no ciberespaço tanto na orientação de guias políticos, processos de tomada de decisão, investimento e conceitos operacionais. Todos esses processos precisam estar alinhados com o ambiente operacional do ciberespaço;
5. Expandir, aprofundar e operacionalizar parcerias. Nessa ação imperativa é exposta a necessidade de atrair talentos para a esfera do Comando Cibernético. Entre os talentos visados para atuar em conjunto com o

> USCYBERCOM estão atores do setor privado, outras agências governamentais, aliados e a academia. Também é salientado o quão importante é o compartilhamento de informação entre esses organismos, o que permite melhor planejamento operacional, desenvolvimento de capacidades e exercícios conjuntos.

De acordo com os Estados Unidos, ao atingir e manter essas ações imperativas, os inimigos do país irão, ao menos, hesitar em confrontá-lo, uma vez que foram estabelecidas inúmeras incertezas (ESTADOS UNIDOS, 2018). As incertezas são aqui compreendidas como possíveis pontos fortes do USCYBERCOM que, em caso de ataques, dificultariam que inimigos obtivessem sucesso em suas empreitadas. Apesar das ações imperativas terem sido divulgadas no ano de 2018, não é possível verificar, de fato, o quão eficientes elas têm sido ao Comando Cibernético estadunidense ou se houve uma diminuição de ataques direcionados à infraestruturas críticas ou informacionais do Estado, uma vez que até então não foi divulgado publicamente nenhum relatório tratando essas questões.

Essa não-divulgação de informações referentes à eficácia do discurso do USCYBERCOM e a ligação disso com uma possível diminuição de ataques cibernéticos certamente serve aos Estados Unidos porque, uma vez que não há divulgação desses dados, não é possível questioná-los. No entanto, tampouco é possível inferir que as cinco ações apresentadas pelo organismo têm, de fato, sido vistas como incertezas a serem inseridas nos cálculos de seus inimigos e/ou diminuído o número de ataques sofridos.

A *National Security Agency* (NSA), por sua vez, é um órgão particular: pertence tanto ao Departamento de Defesa dos Estados Unidos (atuando lado a lado com o USCYBERCOM) como à Comunidade de Inteligência. Apesar de ter a inteligência, interceptação e criptologia como sua missão principal, com o constante crescimento do ciberespaço e nas últimas décadas, a NSA passou a cobrir um papel de importância na alçada cibernética. A segurança cibernética da NSA volta seus esforços para impedir e erradicar ameaças existentes aos sistemas de segurança nacional dos Estados Unidos, focando também na proteção da base industrial de defesa e na melhoria da segurança dos armamentos do país (ESTADOS UNIDOS, 2021).

A NSA representa importância para o USCYBERCOM porque esses dois órgãos estão vinculados desde a criação do Comando Cibernético, o que foi feito para possibilitar que fossem extraídas as práticas utilizadas pela NSA para o USCYBERCOM. Além disso, o fato de o comando das duas instituições estar nas mãos da mesma pessoa, inegavelmente as mantém próximas. O que por um lado é interessante, visto que muitas vezes as responsabilidades e/ou ações desses dois organismos podem se entrelaçar. Mas, por outro lado, existem argumentos para que haja uma separação entre eles, especialmente tendo em vista o caráter militarizado de combate do Comando Cibernético, algo que não é o que se espera da NSA.

Segundo Schoka (2019), apesar da maior parte dos argumentos pró fim da relação entre NSA e USCYBERCOM estarem vinculados ao desenvolvimento bem-sucedido do Comando Cibernético ou ao risco para capacidades e operações da NSA, ainda existe a sobreposição organizacional do USCYBERCOM com a NSA que pode afetar as missões do Comando Cibernético. Conforme o autor, a dependência do Comando Cibernético em relação a NSA molda como o organismo aborda suas operações no ciberespaço.

Tendo em vista os procedimentos e cultura da NSA, Schoka (2019) aponta que o USCYBERCOM se tornou avesso aos riscos inerentes a organizações militares dedicadas a operações ofensivas e que impõem custos à adversários. De fato, argumentos que apontem para o fim do relacionamento entre as duas organizações existem. Seja argumentos que se preocupam com possíveis interferências do USCYBERCOM no ambiente interno via relação com a NSA, seja argumentos que se preocupam com a incapacidade do USCYBERCOM atuar de maneira efetiva em suas missões ofensivas no ciberespaço devido aos procedimentos e cultura da NSA que foram absorvidos pelo órgão. No entanto, é inegável que, para determinados setores do governo estadunidense essa relação tem produzido resultados benéficos, caso contrário ela já teria sido terminada. Ressalta-se que, de forma alguma, esses “resultados benéficos” são necessariamente positivos para a sociedade ou para a governança securitária do ciberespaço estadunidense, apenas quer dizer que essa relação é possivelmente útil a determinados atores.

4.1.2.5 A Governança Securitária do Ciberespaço Estadunidense

Conforme Caballero-Anthony (2019), a governança securitária pode ser representada por processos e arranjos realizados por um conjunto de atores. A governança está presente nos diversos órgãos responsáveis por questões cibernéticas nos Estados Unidos. O *Department of Homeland Security*, por exemplo, destaca na sua discriminação de investimentos parcerias com redes civis e do setor privado para aumentar a segurança de redes críticas (ESTADOS UNIDOS, 2021). Além disso, o órgão também salienta a colaboração com a comunidade responsável por infraestruturas críticas e a importância de existir colaboração, coordenação e cultura de responsabilidades compartilhadas para gerenciar os riscos enfrentados pelas infraestruturas críticas dos Estados Unidos. E é destacado que essas responsabilidades compartilhadas vão desde o nível territorial ao federal.

Entre as instituições dos Estados Unidos, talvez a mais inserida em um sistema de governança securitária voltado para o ciberespaço, seja o FBI. O órgão representa o principal braço investigativo do Departamento de Justiça do país, de forma a investigar os crimes que naturalmente lhe são atribuídos, bem como a fornecer serviços para outros órgãos dos Estados Unidos. De acordo com o FBI (2021), a *National Cyber Investigative Joint Task Force* funciona como um centro cibernético multi-agências. Essa força-tarefa é liderada pelo FBI e possui como membros a *Central Intelligence Agency* (CIA), o *Department of Defense*, *Department of Homeland Security*, a *National Security Agency* (NSA), entre outros (WOODBURN, 2013; ESTADOS UNIDOS, 2021). A atuação dessa força-tarefa foca especificamente na coordenação, integração e compartilhamento de informações relacionadas às investigações de ameaças cibernéticas (ESTADOS UNIDOS, 2021).

O Serviço Secreto dos Estados Unidos, órgão responsável pela proteção do sistema financeiro do país, possui uma força-tarefa similar a do FBI, trabalhando em conjunto com outras agências, bem como com a indústria privada e a academia. Contudo, naturalmente a atuação da *Cyber Fraud Task Forces* é direcionada a lidar com crimes financeiros que possam vir a prejudicar o sistema financeiro dos Estados Unidos.

A Defesa Cibernética dos Estados Unidos, por sua vez, também representa uma estrutura própria de governança securitária voltada para o ciberespaço. Isso ocorre porque o órgão responsável pela Defesa Cibernética no país - o USCYBERCOM -, surgiu vinculado à *National Security Agency* (NSA), inclusive no que diz respeito ao comando dos organismos. O Comando Cibernético é responsável por monitorar, administrar e contra-atacar de forma ofensiva as ameaças cibernéticas que visam prejudicar os Estados Unidos, ao passo que a NSA é responsável pelo monitoramento, coleta e processamento de dados e inteligência tanto a nível doméstico como internacional. Portanto, ao passo que o USCYBERCOM, de fato, atua de forma defensiva e/ou ofensiva contra as ameaças cibernéticas, a NSA fornece as informações necessárias para que a atuação do USCYBERCOM seja a mais bem-informada possível.

Em maior ou menor grau, todos os organismos estadunidenses explorados demonstram que existe ação conjunta com outras agências e/ou instituições para lidar com riscos, crimes, ameaças ou adversidades no ciberespaço. Todavia, não foi possível encontrar uma estrutura única de governança securitária para o ciberespaço estadunidense que envolvesse a todos os organismos de Segurança e Defesa Cibernética ou qualquer forma de hierarquia entre os órgãos. O que existe, de fato, são distintas formas de governança securitária com fins e atores específicos envolvidos, como por exemplo as forças-tarefas voltadas para investigação de crimes cibernéticos ou fraudes financeiras.

4.2 REINO UNIDO E SEUS ORGANISMOS DE SEGURANÇA E DEFESA CIBERNÉTICA

Para discutir a governança securitária do ciberespaço do Reino Unido, serão explorados organismos como MI5, MI6, *Government Communications Headquarters*, *National Cyber Security Centre*, *Cyber and Government Security Directorate* e a *National Cyber Force*. O que se espera, após a análise das funções desses atores, é compreender de que forma eles têm atuado no ciberespaço, bem como entender como eles interagem entre si.

4.2.1 A Inteligência Britânica: MI5, MI6 e o *Government Communications Headquarters* (GCHQ)

MI5 (*Military Intelligence, Section* 5) e MI6 (*Military Intelligence, Section* 6), também conhecidos respectivamente como *The Security Service* e *The Secret Intelligence Service*, são os organismos de inteligência mais conhecidos do Reino Unido. Todavia, trabalhando lado a lado com esses dois órgãos está o *Government Communications Headquarters* (GCHQ), representando, assim, os três principais atores de inteligência britânicos (LERNER, 2004).

A missão do MI5 exposta em sites e documentos oficiais é a de manter o país seguro. O órgão nasceu há mais de um século e tem trabalhado especialmente com ameaças como terrorismo e atividades hostis empregados por atores estatais. Todavia, a partir da ascensão de novas questões na agenda de Segurança Internacional (VILLA, 2017), como o ciberespaço, houve uma reestruturação da organização para que fosse possível lidar com as novas ameaças que chegaram junto a esse domínio.

O Reino Unido destaca que o ciberespaço é descrito como o meio eletrônico com capacidade de armazenar, modificar e comunicar informações, além de incluir a internet e outros sistemas de informação que dão suporte à negócios, infraestruturas e serviços (REINO UNIDO, 2021), definição bastante similar ao que é apresentado por Kuehl (2009) e pela Organização do Tratado do Atlântico Norte (2013 e 2017). Nesse sentido, o país demonstra sua preocupação devido ao fato de que, em maior ou menor medida, a sociedade como um todo depende da disponibilidade desses sistemas regularmente. Portanto, é destacado pelo MI5 a necessidade de que o ciberespaço represente um ambiente seguro, para que a população do Reino Unido, as empresas e os organismos governamentais consigam atuar com o mínimo de riscos nesse domínio.

Entre os atores hostis identificados pelo MI5 que tentam sabotar ou atacar o Reino Unido estão outros Estados, criminosos, grupos de hackers e terroristas (REINO UNIDO, 2021). Algo interessante destacado pelo MI5 é a característica de mudança presente nas capacidades desses diferentes atores, o que faz com que seja necessário atuar e empreender esforços de maneiras distintas quando atuando contra cada um deles. O órgão salienta que,

geralmente, outros Estados possuem melhores capacidades e são equipados de forma mais sofisticada, tornando possível que suas empreitadas sejam bastante perigosas (REINO UNIDO, 2021). Todavia o MI5 destaca que essa não é uma regra excludente: outros atores também podem representar grandes riscos.

O MI5, como dito anteriormente, representa o Serviço de Segurança britânico, o que, em teoria, implicaria que a atuação do órgão ocorresse internamente. No entanto, o Reino Unido destaca que o MI5 é responsável por proteger o país, seus cidadãos e interessantes em território nacional e internacional contra ameaças a segurança nacional (REINO UNIDO, 2021). Por sua vez, a definição de Segurança Nacional do Reino Unido, exposta no segundo capítulo da pesquisa, prevê exatamente a atuação no sentido de proteger o povo, território e interesses britânicos, tanto a nível nacional como internacional. Portanto, é natural que a primeira ameaça identificada pelo organismo seja outros Estados, e o MI5 explicite que é necessário atuar e empreender esforços para lidar com essas ameaças. Portanto, pode-se inferir que o MI5, apesar de ser um órgão de Segurança, atua contra ameaças externas, incluindo outros Estados. Diferentemente do que ocorre no caso dos organismos dos Estados Unidos, a atuação do MI5 contra atores externos está prevista em documentos oficiais e de acordo com as definições adotadas pelo país.

Entre os funcionários do MI5, quando se pensa especificamente a questão cibernética, são apontados os *Cyber Technical Analysts*. São esses especialistas que lideram as investigações contra atores que realizam espionagem sobre o Reino Unido ou tentam sabotar infraestruturas críticas, por exemplo. As formas de trabalho variam desde análises complexas sobre a atuação de atores hostis, desenvolvimento de novas habilidades e a capacidade de investigação (REINO UNIDO, 2021). Esses funcionários, técnicos e especialistas podem, assim como no caso dos especialistas cibernéticos dos Estados Unidos, serem relacionados com a definição de “controladores” de Skinner (2013) e com o componente humano do ciberespaço identificado por Ventre (2012), visto que são esses atores que atuam em nome do Estado no ciberespaço.

O MI6, por sua vez, representa a agência de inteligência que possui a missão de fornecer informações estrangeiras para o governo britânico, ou seja, informações sobre atividades que ocorrem fora do território britânico. Nesse sentido, é esse o órgão que conduz operações secretas fora do Reino Unido e que sistematiza a inteligência para proteger os interesses do país. O MI6 possui quatro principais frentes: 1. combate ao terrorismo internacional; 2. combate à proliferação de armas; 3. apoio à estabilidade no exterior e 4. garantir a vantagem cibernética do Reino Unido (REINO UNIDO, 2021).

Ao se pegar o terceiro ponto exposto pelo Reino Unido: "apoio à estabilidade no exterior", é possível comparar a atuação do Reino Unido com a atuação dos Estados Unidos discutida no segundo capítulo desta pesquisa, a qual destaca a presença militar dos Estados Unidos ao redor do globo para garantir que não ocorram mudanças radicais em balanças de poder existentes. Ou seja, tanto o Reino Unido como os Estados Unidos admitem estar espalhados militarmente pelo mundo para garantir seus interesses e o *status quo* que lhes é favorável. Já o quarto ponto salientado pelo Reino Unido diz respeito a garantir a vantagem cibernética do país em relação aos outros. Nesse sentido, é importante ressaltar que, em 15 de dezembro de 2021, o Reino Unido lançou sua nova Estratégia de Segurança Cibernética 2022, a qual intitula o Reino Unido como uma potência cibernética e estipula os objetivos do país na área cibernética até o ano de 2025. Destaca-se que a Estratégia não foi explorada na presente dissertação tendo em vista sua data de publicação, contudo, será explorada em futuros trabalhos.

Algo enfatizado pelo MI6 é o trabalho conjunto. Especialmente o trabalho realizado com o MI5 e com o *Government Communications Headquarters*, além de outros serviços de segurança e inteligência nacionais e estrangeiros. Destaca-se que, a principal diferença entre MI5 e MI6 se encontra na atuação doméstica e estrangeira: ao passo que o MI5 possui foco de segurança nacional, o MI6 atua reunindo inteligência advinda de fora do território britânico (REINO UNIDO, 2021). Além disso, trabalhando junto a organismos como MI5, GCHQ, *National Cyber Security Centre*, entre outros, o MI6 fornece inteligência para que o Reino Unido consiga atuar da melhor forma possível contra ameaças cibernéticas já existentes e aquelas que ainda estão sendo desenvolvidas (REINO UNIDO, 2021). Aqui é importante ressaltar,

novamente, que apesar do discurso do Reino Unido focar na atuação de segurança do MI5, o país e o próprio organismo identificam outros Estados e atores externos como ameaças à Segurança Nacional e, portanto, colocam o MI5 a disposição para atuar contra tais ameaças.

A atuação do MI6 em relação à cibernética tem o objetivo de "promover e defender o espaço cibernético do Reino Unido usando suas expertises para reduzir ameaças" (REINO UNIDO, 2021, n/p). O foco dessa atuação é identificar riscos e oportunidades no estágio mais breve possível, sempre com o intuito final de que seja possível prevenir as ameaças de se tornarem concretas. A promoção do ciberespaço britânico é algo cada vez mais recorrente no discurso do país, como é possível inferir a partir da Estratégia de Segurança Cibernética 2022 (REINO UNIDO, 2021), a qual categoriza o Reino Unido como uma potência cibernética. Já a atuação do país em relação a identificação de riscos e oportunidades no estágio mais breve possível remete ao conceito de resiliência. O qual prevê aprendizados a partir de falhas, o que é relevante no ciberespaço visto que, muitas vezes, não será possível impedir que atacantes tenham sucesso, portanto é importante aprender onde se errou para que o mesmo erro não volte a acontecer (DEMCHAK, 2012; BRYANT, 2015; PHILLIPS, 2015).

Já o *Government Communications Headquarters* (ou apenas GCHQ) é o órgão de inteligência que, além de fornecer inteligência, protege informações e informantes relevantes para a política do Reino Unido. Entre as capacidades do GCHQ estão: tecnologia de ponta, criatividade e parcerias (como MI5 e MI6) para que ameaças sejam identificadas, analisadas e, em última instância, interrompidas (REINO UNIDO, 2021). Algo a ser destacado é a atuação do GCHQ durante a pandemia de COVID-19 nos anos de 2020 e 2021, o órgão atuou desde o começo da pandemia para fortalecer o sistema de saúde britânico e impedir que possíveis brechas fossem exploradas ou que ataques obtivessem sucesso (REINO UNIDO, 2021).

O organismo foca em desenvolvimento contínuo de suas capacidades com o intuito de tentar estar sempre à frente de ameaças. Esse desenvolvimento contínuo de capacidades é de suma importância no ciberespaço, uma vez que, ao passo que a instituição entende onde falhou, pode corrigir futuros *gaps* de forma a evitar que um ataque seja introduzido da

mesma maneira que ocorreu anteriormente. Como discutido por Kuehl (2009), atores estatais e não-estatais que queira atuar efetivamente no ciberespaço necessitarão superar tecnologias antigas e criar tecnologias novas para, assim, obter vantagem no domínio. Todavia, é impossível se preparar para todas as ameaças existentes, especialmente devido às constantes transformações inerentes ao ciberespaço (SANTOS, 2002; PORTELA, 2018). Contudo, o desenvolvimento contínuo de habilidades, sem dúvida, é necessário para que seja construída uma boa capacidade de resiliência para o Estado no ciberespaço.

Entre as áreas de atuação explicitadas pelo GCHQ estão o contraterrorismo, a segurança cibernética, vantagem estratégica, lidar com crime organizado e o suporte à defesa britânica. Já as capacidades empreendidas pelo órgão são a coleta de dados e análise de comunicação, de dados e de efeitos reais (REINO UNIDO). Por efeitos reais, o órgão especifica a capacidade da sua atuação no ciberespaço obter resultados no mundo real, pode-se pensar no impedimento de um ataque cibernético à alguma infraestrutura crítica de fornecimento de energia, por exemplo. Também se destaca o suporte destacado à defesa britânica, uma vez que o órgão obtém e analisa dados e comunicações vitais para a inteligência e os repassa para os atores os quais tais informações competem.

Todavia, a parte crucial que envolve cibernética pelo GCHQ é o *National Cyber Security Centre* (NCSC), que é parte integrante do organismo. O *National Cyber Security Centre* é um dos órgãos responsáveis por proteger as infraestruturas críticas do Reino Unido de ataques cibernético, além de ser responsável por lidar com os incidentes que de fato chegam a ocorrer e por melhorar a segurança da internet britânica por meio de aconselhamento à cidadãos e organizações e melhoria de tecnologias (REINO UNIDO, 2021).

Institucionalizada em 2016 com o objetivo de fornecer uma resposta unificada a ameaças cibernéticas, e parte integrante do GCHQ, a NCSC é intitulada como a "autoridade técnica" para incidentes cibernéticos (REINO UNIDO, 2021). Destaca-se que a organização surge a partir de quatro organizações prévias: o Grupo de Segurança de Comunicações e Eletrônica; o CERT UK; o Centro de Assessoramento Cibernético e, por fim, o Centro de Proteção de Infraestruturas Críticas Nacionais. Isso é destacado porque, ao

existir quatro organismos prévios à NCSC, torna-se claro que, ao ser institucionalizada, ela já contava tanto com pessoal qualificado, como com conhecimentos, práticas e capacidades pré-existentes, o que pode ter influenciado o seu sucesso.

A gama de atores apoiados pelo NCSC é ampla: infraestruturas e organizações críticas para o Reino Unido, setor público, indústria e até mesmo pequenas e médias empresas. Quando os incidentes de fato ocorrem, o NCSC é acionado e auxilia provendo resposta ao incidente de forma a minimizar os possíveis danos ao país, ajudar o ator que foi atacado a se recuperar (REINO UNIDO, 2021). Ressalta-se, novamente, que os incidentes servem como forma de resiliência, uma vez que o NCSC acaba se aprimorando para futuros ataques. Dificilmente uma organização conseguirá impedir que todos os ataques cibernéticos que a visam ou visam aquilo que a organização protege obtenham sucesso (CHIVVIS; SCHWARZ, 2017), portanto a capacidade de resiliência precisa ser uma prioridade de organismos que lidam com Segurança e Defesa Cibernética para evitar, pelo menos, erros que podem ser aprendidos com experiências prévias.

4.2.2 *National Cyber Force*: a frente unificada da Defesa Cibernética britânica

A *National Cyber Force* (NCF) representa o esforço do Reino Unido em adotar uma frente unificada para lidar com ameaças no ciberespaço, bem como representa a relevância da temática cibernética para o Estado, visto que foi criada uma força específica para lidar com tais ameaças. A NCF é parte integrante de quatro instituições: o Ministério da Defesa, o Laboratório de Ciência e Tecnologia de Defesa, o Serviço Secreto de Inteligência e o *Government Communications Headquarters* (GCHQ), de forma a estabelecer uma parceria ativa entre a Defesa e a Inteligência britânica (REINO UNIDO, 2021).

Entre as responsabilidades atribuídas à NCF estão operações por meio do ciberespaço para conter ameaças, impedir as ações daqueles que tentem atacar o Reino Unido ou países aliados, manter o Estado seguro e, ainda, promover interesses britânicos tanto a nível nacional como internacional (REINO UNIDO, 2021). Após a criação da *National Cyber Force*, que ocorreu

em 2020, em março de 2021 o governo do Reino Unido publicou a *Integrated Review of Security, Defence, Development and Foreign Policy*, a qual representa o documento que estabelece a visão de futuro da Segurança e Defesa britânica até o ano de 2031.

Por meio da *Integrated Review*, o governo britânico reconhece as constantes mudanças nas mais diversas áreas: sociedade, economia, governo (incluindo a defesa), leis e política externa, devido às peculiaridades do espaço cibernético. Mudanças essas que representam, também, ameaças e vulnerabilidades com as quais o Estado precisa se preparar para lidar (CASHELL et al., 2004; TURK, 2005; DEVANNY et al., 2020). Ademais, o documento posiciona o Reino Unido como uma potência cibernética, sendo capaz de proteger e promover seus interesses via ciberespaço e estabelece que o Estado utilizará operações cibernéticas como parte de suas missões econômicas, militares e diplomáticas. A discurso do Reino Unido, ao se posicionar como uma potência cibernética e explicitar que irá promover diversos interesses por meio do ciberespaço é notável. De fato, o país se encontra na terceira posição entre os trinta países com mais poder no espaço cibernético conforme ranking divulgado pelo *Belfer Center for Science and International Affairs* em 2020 (VOO et al., 2020) e o discurso do Reino Unido demonstra que o país fará uso de suas capacidades cibernéticas para atingir seus objetivos, sejam eles econômicos, militares ou diplomáticos.

Por fim, devido ao fato de que é um organismo misto (orquestrado por instituições de Inteligência e Defesa), a *accountability*, ou seja, a responsividade (SCHEDLER, 1999; RODRIGUES, 2020) das atividades empregadas pela *National Cyber Force*, recaem tanto sobre o *Secretary of State for Foreign, Commonwealth and Development Affairs*, como sobre o *Secretary of State for Defence*. Além disso, há uma estrutura legal que norteia as atividades conduzidas pela National Cyber Force de acordo com leis internacionais e do Reino Unido (REINO UNIDO, 2021). É preciso salientar que a *National Cyber Force* representa um organismo recente, tendo sido estabelecido no ano de 2020. Todavia, o Reino Unido tem dado atenção significativa ao organismo, inclusive via investimento, que ultrapassará 5 bilhões de libras até o ano de 2030, segundo a BBC (2021). Soma-se a isso o fato da Força Cibernética Nacional representar um organismo híbrido, o qual

trabalha tanto na frente e segurança e inteligência, como na frente específica de defesa, o que, possivelmente, permitirá que haja coordenação, responsabilização e atribuição de ações.

4.2.3 A Governança Securitária do Ciberespaço Britânico

Conforme Krahmann (2005), a governança securitária surge para que um conjunto de atores consiga coordenar suas necessidades e interesses sobre determinada temática. Essa atuação conjunta se mostra muito presente na realidade britânica no ciberespaço. Sem exceção, todos os organismos analisados no presente estudo de caso (MI5, MI6, GCHQ, NCSC, NCF), em maior ou menor medida, discutem a importância do relacionamento com outras instituições para atingir a melhor atuação no ciberespaço.

O Serviço de Segurança (MI5) salienta a atuação em conjunto com os outros órgãos de inteligência: MI6 e *Government Communications Headquarters*. Essa relação entre os organismos é interessante, especialmente quando se pensa o escopo de atuação de cada órgão: a jurisdição do MI5, por exemplo, permite apenas que ele atue tanto internamente como externamente, diferentemente do MI6, que possui atribuições extraterritoriais. Portanto, a proximidade entre esses órgãos é saudável para a Segurança Cibernética britânica porque, uma vez que for identificado alguma atividade ilegal ou ameaça pelo MI5 que esteja vindo de fora do território nacional e que seja melhor atribuída ao MI6, o órgão pode encaminhar toda a informação relevante para o MI6 atuar em tempo real revido a relação existente entre os dois.

A governança realizada pelo MI6 é ainda mais ampla do que aquela do MI5: o órgão, assim como o MI5, atua em conjunto com outras instituições de Inteligência e Defesa nacionais, porém, atua também em conjunto com serviços de segurança e inteligência internacionais. Dessa forma, o MI6 permite ao Reino Unido a vantagem de obter informações que, talvez, não seriam obtidas caso não houvesse o compartilhamento por agências de outros Estados. Todavia, é necessário ter em mente que essa relação exige confiança entre todas as partes, portanto é possível que isso ocorra apenas com países aliados, como é o caso da relação entre os Estados-membro da Organização do Tratado Atlântico Norte, a qual possui Estados Unidos e Reino Unido como

membros. Ademais, mesmo existindo essa relação entre países aliados, soma-se o fato de interesses individuais no ciberespaço e no sistema internacional (WALTZ, 1979; WARREN, 1992, MEARSHEIMER, 2001), portanto nem sempre as informações serão compartilhadas, apesar de haver alianças fortes.

Um exemplo peculiar da governança securitária voltada para o ciberespaço do Reino Unido é a institucionalização do *National Cyber Security Centre* em 2016. Esse organismo é o ator central no combate às ameaças cibernéticas que visam as infraestruturas críticas do Reino Unido (REINO UNIDO, 2021). Essa instituição é especial para a governança securitária do ciberespaço britânico porque, como dito anteriormente, ela surge, justamente, da junção de quatro organismos pré-existentes: o CERT UK; o Centro de Assessoramento Cibernético e, por fim, o Centro de Proteção de Infraestruturas Críticas Nacionais. Essa institucionalização a partir de quatro órgãos que já estavam em plena operacionalização permitiu que a NCSC contasse com um quadro de funcionários especializado desde a sua criação.

Por fim, e talvez representando o maior ato da governança securitária do ciberespaço britânico, surge em 2020 a *National Cyber Force*. O órgão representa a unificação da Inteligência e Defesa britânica em um só lugar com o intuito de conter e impedir ações e ameaças no ciberespaço que representem risco ao Reino Unido, bem como com o intuito de promover os interesses do Reino Unido no ciberespaço.

A criação da National Cyber Force vai de encontro ao lançamento de dois documentos oficiais britânicos: a *Integrated Review of Security, Defence, Development and Foreign Policy* (2021) e a *National Cyber Strategy* 2022, lançada em dezembro de 2021. Ambos os documentos destacam o Reino Unido como uma potência cibernética e focam na sua atuação no ciberespaço nas mais diversas esferas: social, econômica, militar. Nesse sentido, a *National Cyber Force* se consolida como o organismo que irá representar o Reino Unido no ciberespaço de forma a lidar com possíveis ameaças, bem como a projetar o Estado como potência cibernética.

5 CONSIDERAÇÕES FINAIS

A construção da presente dissertação se insere em um contexto internacional no qual cada vez mais organizações, partes dos setores público e privado, Estados e suas respectivas populações, estão, em maior ou menor grau, vinculados ao ciberespaço. A partir da constante inserção de usuários neste domínio, são identificados riscos, ameaças e também pontos a serem explorados por diversos atores com agendas distintas. Nesse sentido, buscou-se contribuir com a agenda de pesquisa referente à área de Segurança e Defesa Cibernética. Para auxiliar o desenvolvimento da pesquisa, foram elaboradas duas preposições e um problema de pesquisa, que serão explorados nesta seção final.

Ao decorrer do primeiro capítulo, buscou-se explorar e analisar conceitos basilares para o trabalho como um todo. Entre os conceitos estão Governança, Governança Securitária, Ciberespaço, Poder e Poder Cibernético. Além disso, foram trabalhadas questões referentes ao Sistema Internacional, como o impacto do final da Guerra Fria na mudança da agenda securitária dos Estados sobre o que é considerado ameaça.

Foram exploradas diversas conceituações de Governança (Yong e Wenhao, 2012; Fukuyama, 2013; Mello e Slomski, 2010; Farrington, 2009; Oliveira e Pisa, 2015). E a conclusão a que se chegou foi de que o conceito de Governança seria entendido, na presente dissertação, como a coordenação da ação e tomada de decisão entre sociedade, atores estatais e não-estatais sobre determinado assunto. Diferentemente do que acontece no caso do conceito de Governança, que possui definições bastante distintas entre si, o conceito de Governança Securitária é mais coeso entre os autores que o trabalham.

Logicamente existem distinções no conceito de Governança Securitária, mas os elementos comuns na definição se sobressaem. Como por exemplo a multiplicidade de atores; a coordenação de forma não-hierárquica e a combinação de mecanismos formais e informais na ação e tomada de decisão (KRAHMANN, 2003; WEBBER et. al, 2004; KIRCHNER, 2006; FLEMES; RADSECK, 2009; CABALLERO-ANTHONY, 2019). É importante ressaltar, mais uma vez, que o conceito de governança securitária prevê a coordenação

entre atores estatais e não-estatais, contudo, devido ao limite de tempo para a realização da dissertação foram analisados apenas organismos estatais de Segurança e Defesa Cibernética. Espera-se que, em futuros trabalhos, a análise seja expandida de forma a incluir atores não-estatais responsáveis por lidar com questões cibernéticas.

O conceito de Ciberespaço também possui significados extremamente distintos entre si. Portanto, após analisar as definições de diversos autores (PARKER, 1993; KUEHL, 2009; LIBICKI, 2009; RATTRAY, 2009; SHELDON, 2011; VENTRE, 2012; REINO UNIDO, 2016; OTAN, 2017; ESTADOS UNIDOS, 2021), optou-se por definir o conceito de forma a adequá-lo ao trabalho. Nesse sentido, o ciberespaço é compreendido como um domínio composto por três camadas: física, sintática e humana. A camada física representa o componente tangível do ciberespaço, como os cabos submarinos, satélites e todo *hardware* em geral; a camada sintática diz respeito ao *software*, às instruções enviadas às máquinas e a comunicação própria que ocorre entre as redes computadorizadas e, por fim, a camada humana representa o tomador de decisão no ciberespaço, bem como o componente cognitivo que constrói esse domínio diariamente.

Assim como a maioria dos conceitos discutidos no primeiro capítulo, o conceito de Poder Cibernético não foge da regra de possuir distinções entre suas definições. Willett (2019) discorre sobre como essa forma de poder não possui apenas caráter militar, e sim é multifacetado. Isso porque é envolvido com questões financeiras, de infraestruturas críticas, segurança e defesa cibernética, entre outras. Kuehl (2009) traz para a discussão sobre o conceito de Poder Cibernético a variável de que, os propósitos e humanos do poder cibernético serão moldados de acordo com a missão da instituição que o utiliza, seja ela militar, econômica ou política. O que, de certa forma, valida o argumento de Willett (2019) como essa forma de poder é multifacetada.

Por fim, também é trabalhado no primeiro capítulo a forma como o Sistema Internacional foi impactado com o pós Guerra Fria. Durante o período da Guerra Fria, os objetivos de segurança dos Estados claramente estavam voltados para fins militares e de guerra convencional, visto que essa era a ameaça existente seja para a frente soviética, seja para a frente estadunidense. Todavia, com o fim da Guerra Fria, houve uma expansão da

agenda de segurança, na qual foram inseridos novos temas, como migração, questões ambientais e, eventualmente, questões cibernéticas.

O segundo capítulo da pesquisa, por sua vez, foca em analisar conceitos como Segurança, Segurança Nacional, Defesa, Defesa Cibernética e Segurança Cibernética. Além de fontes acadêmicas, buscou-se, sempre que possível, trabalhar com as conceituações expostas por Estados Unidos e Reino Unido, para que fosse possível estabelecer um *link* no último capítulo entre as definições empregadas aos conceitos pelos países e as atribuições que são dadas aos seus organismos de Segurança e Defesa Cibernética.

Assim como no caso do conceito de Ciberespaço, o qual foi adequado à pesquisa, após analisar as definições acadêmicas e estatais sobre Segurança Cibernética e Defesa Cibernética atribuiu-se uma definição própria aos termos. A Segurança Cibernética, por exemplo, passou a ser compreendida como a capacidade de proteção dos sistemas conectados à internet e das informações e dados contidos nesses sistemas, bem como das camadas vinculadas ao ciberespaço, seja *hardware*, seja *software* ou *peopleware.* E, em um sentido mais amplo, a Segurança Cibernética representa a capacidade de assegurar o mantenimento da sociedade da informação de um país no ciberespaço.

A Defesa Cibernética, por sua vez, é compreendida como o conjunto de ações ofensivas, defensivas e exploratórias realizadas por Estados no ciberespaço com o objetivo de proteger seus sistemas de informação, suas infraestruturas críticas e, em um sentido mais amplo, a própria soberania do Estado. As ações de Defesa Cibernética visam, dessa forma, proteger o Estado de quaisquer ameaças ou possibilidades de ameaça e incluem a detecção, caracterização, combate e mitigação dessas ameaças, além da capacidade de restauração daquilo que for danificado o mais breve possível.

Entre as descobertas da presente pesquisa, se destaca o fato de não haver nos Estados Unidos ou no Reino Unido, uma estrutura de governança securitária do ciberespaço única para lidar com Segurança e Defesa Cibernética. O que existe, na verdade, são governanças securitárias voltadas para questões específicas de Segurança ou Defesa Cibernética, como é o caso da *Cyber Fraud Task Forces* (CFTFs) nos Estados Unidos. Essa força-tarefa representa, portanto, uma estrutura de organismos voltados especificamente

para lidar com prevenção, detenção, mitigação e investigação de crimes financeiros no ciberespaço.

As infraestruturas críticas representam um ponto de enorme relevância para ambos os Estados em análise. No caso dos Estados Unidos, se torna perceptível a importância da proteção de IFCs por meio da institucionalização da *Cybersecurity and Infrastructure Security Agency* (CISA), que obteve um orçamento de cerca de 1.8 bilhão em 2021. Esse órgão, subordinado ao *Department of Homeland Security*, possui como objetivo primordial a segurança, assistência em caso de ataques e investigação de ataques cibernéticos direcionados à Infraestruturas Críticas.

O Reino Unido, por sua vez, possui sua própria instituição voltada para garantir a segurança de suas infraestruturas críticas: o *National Cyber Security Centre*, estabelecido em 2016. Além disso, esse organismo em si representa, de certa forma, uma estrutura de governança securitária. Isso ocorre porque ele foi criado a partir da reunião de três organismos em um, sendo esses organismos o CERT UK, o Centro de Assessoramento Cibernético e o Centro de Proteção de Infraestruturas Críticas. Com isso, foi possível trazer o conhecimento e o pessoal já existente de três instituições para uma única instituição que tem como objetivo proteger as Infraestruturas Críticas do Reino Unido e garantir a melhor resiliência possível para quando ataques cibernéticos tenham sucesso em penetrá-las.

A governança securitária existente entre os órgãos responsáveis pela Defesa Cibernética de ambos os países com instituições/agências de inteligência também chama a atenção. No caso do Comando Cibernético dos Estados Unidos (USCYBERCOM), por exemplo, tem-se um vínculo com a *National Security Agency* (NSA), ao passo que a Força Cibernética Nacional do Reino Unido (*National Cyber Force*), representa uma força híbrida entre organismos de inteligência e de defesa britânicos.

Esse vínculo entre Defesa e Inteligência, por um lado, é interessante, porque permite que a Defesa possua acesso a capacidades, informações e técnicas que talvez não teria se não houvesse a ligação com esses órgãos de inteligência. Contudo, por outro lado, uma vez que a Defesa Cibernética se encontra tão interligada a organismos de inteligência, é preciso que se considere a atuação doméstica dessas instituições, como é o caso do MI5 no

Reino Unido, de forma que se evite a utilização de instituições de Defesa para retaliar ou atacar atores domésticos e que sejam mantidas as funções da Defesa para lidar com ameaças/atores externos.

A descoberta que se julga mais crucial, no entanto, diz respeito à atuação dos organismos de Segurança dos Estados Unidos. Diferentemente do que ocorre no Reino Unido, alguns dos organismos responsáveis por lidar com questões cibernéticas nos Estados Unidos (como por exemplo o DHS, a CISA e o FBI), apesar de representarem organismos de Segurança, possuem atribuições típicas de Defesa. Entre essas atribuições, encontra-se o enfrentamento de ameaças externas via ações ofensivas no ciberespaço, por exemplo. Essa atuação dos organismos de segurança dos Estados Unidos vai contra, inclusive, o que está disposto em documentos oficiais referente às definições de Segurança e Segurança Cibernética do país.

Um conceito que foi encontrado na reta final da dissertação e, por isso, não foi explorado no capítulo teórico-conceitual, é o conceito de *Gray Zone*. Essa chamada zona cinzenta representa, conforme apontado por Wirtz (2017), os confrontos que ocorrem na extremidade inferior do "espectro de conflito em que a guerra ainda não está em andamento, mas a coerção militar está ocorrendo para alterar o *status quo"* (WIRTZ, 2017, p. 106). Especula-se que, possivelmente, ações de Segurança e Defesa Cibernética, como as ações ofensivas empregadas pelos organismos dos Estados Unidos e Reino Unido previamente apresentadas previamente, possam ocorrer nessa extremidade do conflito onde ainda não é considerado guerra, mas existem forças alterando o *status quo*. Portanto, o que se pretende é que, em trabalhos futuros, seja aprofundada a relação entre o conceito de *Gray Zone* e a atuação de atores securitários do ciberespaço.

A seguir, são discutidos o pressuposto da pesquisa e as duas preposições levantadas no começo da pesquisa, bem como é respondido o problema de pesquisa.

Pressuposto 1: a estruturação da governança securitária de um Estado está diretamente relacionada às ações de Defesa Cibernética e de Segurança Cibernética deste Estado.

Com base no que foi descoberto ao longo do trabalho, especialmente nos estudos de caso de Estados Unidos e Reino Unido no capítulo quatro, esse

pressuposto se mantém. É possível inferir, a partir dos estudos de caso, que a estrutura de governança securitária do ciberespaço do Estado está relacionada às ações de Defesa Cibernética e Segurança Cibernética empregadas por esse Estado, tendo em vista que foram encontradas estruturas de governança securitária organizadas para lidar com distintas ameaças no domínio cibernético, tanto no caso dos Estados Unidos como no caso do Reino Unido.

Preposição 1: a governança securitária do ciberespaço influencia o processo de securitização deste domínio.

Não foi possível comprovar a preposição de que a governança securitária do ciberespaço influencia o processo de securitização deste domínio. A agenda em torno do ciberespaço definitivamente tem passado por processos de securitização, isso fica claro ao passo que vemos o empenho de países como Estados Unidos e Reino Unido para lidar com questões de Segurança e Defesa Cibernética. Todavia, tendo em vista que nos casos de Estados Unidos e Reino Unido foram encontradas estruturas de governança securitária cibernética voltadas para diferentes questões e não apenas uma governança estruturada de forma hierárquica, não é possível inferir que é a governança que influencia o processo de securitização, apesar de estar claro que o ciberespaço tem sido securitizado.

Preposição 2: a escolha de utilização dos termos Segurança Cibernética ou Defesa Cibernética feita por um Estado, em documentos oficiais de Defesa, reflete a forma na qual este Estado irá responder às ameaças no ciberespaço.

A segunda e última preposição foi parcialmente rejeitada. Isso ocorre porque, no caso dos Estados Unidos, foram identificados organismos de Segurança que, claramente, possuem atribuições típicas de Defesa. Entre esses organismos estão o *Federal Bureau of Investigation* (FBI), o *Department of Homeland Security* (DHS) e a *Cybersecurity and Infrastructure Security Agency* (CISA). A CISA, por exemplo, emprega ações ofensivas contra ameaças cibernéticas às infraestruturas críticas dos Estados Unidos, apesar de ser uma agência de segurança. Já o DHS aponta, entre seus quatro principais objetivos, que o órgão é responsável por coordenar a resposta a ataques cibernéticos significativos.

O discurso do FBI é o mais assertivo entre os organismos estadunidenses: o órgão destaca que irá impor riscos e consequências aos

seus inimigos no espaço cibernético e, além disso, discorre sobre a sua capacidade de alterar o comportamento de atores criminosos estatais e não-estatais, de forma a fazer com que esses atores repensem qualquer ato contra os Estados Unidos. Posto isso, fica claro que existe um transbordamento na atuação dos organismos de Segurança Cibernética no caso dos Estados Unidos, uma vez que a ação desses atores no ciberespaço não corresponde, inclusive, ao que é disposto sobre Segurança e Segurança Cibernética em documentos oficiais do país.

É necessário enfatizar que as duas preposições foram respondidas com base no conjunto de dados e informações coletados ao longo da pesquisa, por meio de fontes acadêmico-científicas, fontes primárias (documentos e declarações oficiais de Estado) e informações jornalísticas. Não foram conduzidas entrevistas e/ou realizadas viagens de campo para colocá-las à prova.

Tem-se o seguinte problema de pesquisa: de que forma a estrutura de governança securitária do ciberespaço de um Estado pode afetar ações de Defesa Cibernética e de Segurança Cibernética?

Foi possível observar, com base nos estudos de caso de Estados Unidos e Reino Unido, que estruturas de governança securitária são úteis, no ciberespaço, para lidar com ameaças/riscos específicos. Não foi identificado, em nenhum dos casos, uma estrutura de governança securitária que estabelecesse qualquer forma de ligação entre todos os organismos de Segurança e Defesa Cibernética, ou qualquer hierarquia entre eles. O que foi encontrado, na verdade, foram governanças securitárias com fins específicos no ciberespaço: como a proteção de infraestruturas críticas (responsabilidade da CISA nos Estados Unidos e da NCSC no Reino Unido); a proteção de sistemas financeiros (que ocorre nos Estados Unidos via *Cyber Fraud Task Forces* do Serviço Secreto em conjunto com outras agências).

Além disso, foi possível identificar, em ambos os casos, a existência de forte vínculo da Defesa Cibernética com organismos de segurança. O caso dos Estados Unidos é mais emblemático porque, desde a criação do Comando Cibernético, em 2009, o organismo é subordinado ao mesmo comandante da *National Security Agency* (NSA). Essa relação se deu, de acordo com os Estados Unidos (2018 e 2021), para que fosse possível que o Comando

Cibernético absorvesse as experiências e capacidades da NSA. Todavia, mesmo após isso ter sido cumprido, a relação entre as duas frentes não deixou de existir, o que gera questionamentos sobre possíveis interesses da Defesa estadunidense em relação a atuação em ambiente interno, o que pode ser facilitado via relação com a NSA.

No caso do Reino Unido, a relação entre Segurança e Defesa Cibernética se tornou mais forte recentemente, com a criação da *National Cyber Force* (NCF) em 2020. O intuito da NCF, como exposto em documentos oficiais, é que seja adotada uma frente unificada para lidar com as ameaças cibernéticas, sejam essas ameaças de segurança ou defesa. Portanto, para garantir uma atuação contínua, a NCF faz parte de quatro instituições: o Ministério da Defesa, o Laboratório de Ciência e Tecnologia de Defesa, o Serviço Secreto de Inteligência e o *Government Communications Headquarters* (GCHQ) (REINO UNIDO, 2021). Dessa forma, as atribuições da Força não se restringem apenas à área de Segurança ou Defesa, é possível atuar em ambas. Outro ponto a ser salientado sobre a NCF, é a forma como o Reino Unido tem construído o discurso em torno dela: o país se coloca na posição de potência cibernética em documentos recentes (*Integrated Review, 2018; National Cyber Strategy, 2022*). E, como potência cibernética, o Reino Unido destaca que irá utilizar operações cibernéticas para atingir seus objetivos, sejam eles militares, econômicos ou diplomáticos, sendo a NCF a principal instituição nessa frente.

Portanto, com base no que foi visto nos casos de Estados Unidos e Reino Unido, foi possível observar que, em alguns casos, estruturas de governança securitária voltadas para questões cibernéticas podem afetar ações de Defesa Cibernética e Segurança Cibernética, como visto por meio da atuação da *Cyber Fraud Task Forces* nos Estados Unidos, por exemplo, que representa uma governança securitária com ações específicas para conter crimes financeiros. Ou o caso dos órgãos responsáveis por lidar com ameaças às infraestruturas críticas tanto no caso dos Estados Unidos como no caso do Reino Unido, nos quais são formadas governanças securitárias com o objetivo específico de defender as infraestruturas críticas dos países.

Contudo, para afirmar que a estrutura de governança securitária do ciberespaço de um Estado, como um todo, pode afetar ações de Defesa

Cibernética e Segurança Cibernética ainda é preciso verificar informações que não foram abordadas ou aprofundadas na presente dissertação devido ao limite de tempo para a realização do trabalho. Todavia, a intenção é que a agenda de pesquisa referente a governança securitária do ciberespaço seja mantida ao longo dos próximos anos, o que, esperançosamente, permitirá desvendar informações que não foram encontradas na pesquisa até o presente momento.

REFERÊNCIAS

ABDENUR, A. Brazil and Cybersecurity in the Aftermath of the Snowden Revelations. **International Security: a European-South American Dialogue,** p. 229-283, 2014.

ALSINA JR, J. P. S. A síntese imperfeita: articulação entre política externa e política de defesa na era Cardoso. **Revista Brasileira de Política Internacional,** v. 46, n. 2, p. 53-86, 2003.

AMORIM, C. Defesa nacional e pensamento estratégico brasileiro. **Revista política hoje**, v. 21, n. 2, 2012.

ARQUILLA, J.; RONFELDT, D. **Networks and netwars: The future of terror, crime, and militancy.** Rand Corporation, 2001.

ÁTRIA, R, B. **Libros de defensa: Una base común para su elaboración.** In: Pachedo Gaitán, Guillermo (ed). Políticas de defensa y elaboración de libros blancos. Experiencias latinoamericanas. Santiago, Chile, 2003, p. 18 13-25 242 p.

BALDWIN, D. A. The concept of security. **Review of International Studies,** v. 23, n. 1, 1997, p. 5-26.

BBC. **National Cyber Force to be based in Samlesbury**. Disponível em: https://www.bbc.com/news/uk-england-lancashire-58779337. Acesso em: 26 nov. 2021.

BEHAR, D. **Evolución de la Ciber Seguridad Moderna.** 2016. Disponível em: https://www.sites.oas.org/cyber/Documents/2016%20-%20Evolucio%CC%81n%20de%20la%20Ciberseguridad%20moderna%20y%20sus%20desafios%20a%20trave%CC%81s%20de%20la%20historia-Daniel%20Behar.pdf. Acesso em: 01 mar. 2021.

BRODIE, B. **National security policy and economic stability**. Yale Institute of International Studies, 1950.

BROOKS, S. G. Dueling realisms. **International Organization,** p. 445-477, 1997.

BRASIL. **Doutrina Militar de Defesa Cibernética.** 2014.

BRASIL. **Estratégia Nacional de Defesa.** Brasília: Presidência da República, 2008.

BRASIL. **Estratégia Nacional de Defesa.** Brasília: Presidência da República, 2020.

BRASIL. **Glossário das Forças Armadas.** 2015. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 01 mar. 2021.

BREWER, S, E. Structural human rights violations: The true face of Mexico's war on crime. **Human Rights Brief**, v. 16, n. 2, p. 2, 2009.

BRUNNER, E. M.; CAVELTY, M. D. The formation of in-formation by the US military: Articulation and enactment of infomanic threat imaginaries on the immaterial battlefield of perception. **Cambridge Review of International Affairs**, v. 22, n. 4, p. 629-646, 2009.

BRYANT, W. D. Resiliency in future cyber combat. **Strategic studies quarterly**, v. 9, n. 4, p. 87-107, 2015.

BULL, H. **The anarchical society**: A study of order in world politics. London: Macmillan. 1977.

BUZAN, B. et al. **Security: A new framework for analysis.** Lynne Rienner Publishers, 1998.

BUZAN, B. New patterns of global security in the twenty-first century. **International affairs,** v. 67, n. 3, p. 431-451, 1991.

CABALLERO-ANTHONY, M. Security Governance and ASEAN's Political Security Community: Fragmented but Inclusive Security Communities?. **Fudan Journal of the Humanities and Social Sciences,** v. 13, n. 1, p. 151-167, 2020.

CAMPBELL, D. Cultural governance and pictorial resistance: reflections on the imaging of war. **Review of International Studies**, v. 29, p. 57-73, 2003.

CARVALHO, P. S. M. **O setor cibernético nas Forças Armadas brasileiras**. Brasília: Forense, 2011.

CARR, E, H. (2001). **Vinte anos de crise: 1919-1939.** Brasília: Universidade de Brasília e Instituto de Pesquisa de Relações Internacionais.

CASHELL, B. et al. The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC), v. 2, 2004.

CAVAGNARI, F. "América do Sul: Alguns Subsídios para Definição da Segurança Nacional". ["**South America: Some Inputs for the Definition of National Security**"]. 1994.

CAVELTY, M. D. Cyber-Security**. The Routledge Handbook of New Security Studies Routledge**. 2010.

CAVELTY, M. D. **The militarisation of cyberspace:** Why less may be better. In: 2012 4th international conference on cyber conflict (CYCON 2012). IEEE, 2012. p. 1-13.

CEPIK, Marco. **Segurança Nacional e Segurança Humana: problemas conceituais e consequências políticas,** 1. 2001.

CEPIK, M. Segurança Internacional: da Ordem Internacional aos desafios para a América do Sul e para a CELAC. **SORIA, AB; ECHANDI, IA Desafios estratégicos del regionalismo contemporáneo CELAC e,** 2013.

CHIVVIS, C. S.; DION-SCHWARZ, C. **Why It's So Hard to Stop a Cyberattack — and Even Harder to Fight Back**. 2017. Disponível em: https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html. Acesso em: 26 nov. 2021.

COSTA, D. Segurança e defesa: uma única visão abaixo do Equador. **Revista Brasileira de Política Internacional,** v. 42, n. 1, p. 127-156, 1999.

DEMCHAK, C. C.; DOMBROWSKI, P. Rise of a cybered westphalian age. **Strategic Studies Quarterly,** v. 5, n. 1, p. 32-61, 2011.

DEMCHAK, C. C. Resilience and cyberspace: Recognizing the challenges of a global socio-cyber infrastructure (gsci). **Journal of Comparative Policy Analysis: Research and Practice,** v. 14, n. 3, p. 254-269, 2012.

DEVANNY, Joseph; GOLDONI, Luiz Rogério Franco; MEDEIROS, Breno Pauli. The 2019 Venezuelan blackout and the consequences of cyber uncertainty. **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, 2020.

DE ARAÚJO, J. Estados Unidos, poder cibernético e a "guerra cibernética": Do Worm Stuxnet ao Malware Flame/Skywiper–e além. **Boletim Meridiano,** v. 47, 2012.

DEWAR, R. S. The "triptych of cyber security": A classification of active cyber defence. In: **2014 6th International Conference On Cyber Conflict (CyCon 2014).** IEEE, 2014. p. 7-21.

DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing Cyber Security in Brazil: threats and responses. Igarapé Institute**,** Rio de Janeiro, **Strategic Paper** 11, p. 1-35, Dez. 2014.

FARRINGTON, C. Putting good governance into practice I: the Ibrahim Index of African Governance. **Progress in development studies**, v. 9, n. 3, p. 249-255, 2009.

FERNANDES, J. P. T. **A ciberguerra como nova dimensão de conflitos do século XXI.** Relações Internacionais, v. 33, p. 53-69, 2012.

FERREIRA NETO, W. B. Territorializando o "Novo" e (Re) territorializando os Tradicionais: a cibernética Como Espaço e Recurso de Poder. **Segurança e Defesa Cibernética: da fronteira física aos muros virtuais,** 2014.

FLEMES, D.; RADSECK, M. **Creating multilevel security governance in South America**. 2009.

FLYVBJERG, B. **Five Misunderstaindings about case-study research.** 2006.

FUCCILLE, A.; REZENDE, L. P. Complexo regional de segurança da América do Sul: uma nova perspectiva. **Contexto Internacional**, v. 35, n. 1, p. 77-104, 2013.

FUKUYAMA, F. What is Governance? **Governance**, v. 26, n. 3, p. 347-368, 2013.

GALINEC, D.; MOŽNIK, D.; GUBERINA, B. Cybersecurity and cyber defence: national level strategic approach. **Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije,** v. 58, n. 3, p. 273-286, 2017.

GEORGE, A. L. et al. **Case studies and theory development in the social sciences.** mit Press, 2005.
GIL, A, C. **Métodos e técnicas de pesquisa social.** 6. ed. Editora Atlas SA, 2008.

GOLDSMITH, J. How cyber changes the laws of war. **European Journal of International Law,** v. 24, n. 1, p. 129-138, 2013.

GONZALES, S. L. M.; PORTELA, L. S. THE GEOPOLITICS OF THE SOUTH AMERICAN CYBERNETIC SPACE: THE (NON) SHAPING OF SECURITY POLICIES AND CYBERNETIC DEFENSE? 1. **AUSTRAL: Brazilian Journal of Strategy & International Relations,** v. 7, n. 14, 2018.

GOODRICK, D. et al. Comparative case studies: **Methodological briefs-impact evaluation** no. 9. 2014.

GUEDES, M. A. et al. **Guia de defesa cibernética na América do Sul.** Recife: Editora UFPE, 2017. Disponível em: https://pandia.defesa.gov.br/pt/acervo-digital/35-programa-%C3%A1lvaro-alberto-de-indu%C3%A7%C3%A3o-%C3%A0-pesquisa-em-defesa-nacional-e-seguran%C3%A7a-internacional/826-guia-de-defesa-cibern%C3%A9tica-na-am%C3%A9rica-do-sul,-por-marcos-aurelio-guedes-et-al. Acesso em: 01 mar. 2021.

GUITTON, C.; KORZAK, E. The sophistication criterion for attribution: Identifying the perpetrators of cyber-attacks. **The RUSI Journal**, v. 158, n. 4, p. 62-68, 2013.

HANSEN, L; NISSENBAUM, H. Digital disaster, cyber security, and the Copenhagen School. **International studies quarterly,** v. 53, n. 4, p. 1155-1175, 2009.

HAUBEN, M. **History of ARPANET**. Site de l'Instituto Superior de Engenharia do Porto, v. 17, 2007.

HEGEN, D. **Aspects of the Cybersecurity Ecosystem in the United States**. 2020. Disponível em: https://www.kas.de/documents/252038/7938566/Aspects+of+the+Cybersecurity+Ecosystem+in+the+United+States.pdf/444bfa30-7e00-e870-f8a4-f3310a805635?version=1.0&t=1592898343203. Acesso em: 26 nov. 2021.

HERZ, M. Concepts of security in South America. **International Peacekeeping,** v. 17, n. 5, p. 598-612, 2010.

HOBBES, T. **Leviatã.** Clube de Autores, 2020.

KEOHANE, R, O.; JOSEPH, S. NYE. (1977) Power and Interdependence: World Politics in Transition. **Glenview, IL: Scott, Foresman and Company**.

KIRCHNER, E. J. European Security Trends. **Jean Monnet/Robert Schuman Paper Series,** Vol. 3 No. 6, September 2003. 2003.

KIRCHNER, E. J.; DOMINGUEZ, R. Security governance in a comparative regional perspective. **European security,** v. 23, n. 2, p. 163-178, 2014.

KLIMBURG, A; FAESEN, L. A Balance of Power in Cyberspace. **Governing Cyberspace,** p. 145, 2020.

KRAHMANN, E. Conceptualizing security governance. **Cooperation and conflict,** v. 38, n. 1, p. 5-26, 2003.

KRAHMANN, E. Security governance and networks: New theoretical perspectives in transatlantic security. **Cambridge review of international affairs,** v. 18, n. 1, p. 15-30, 2005.

KRAHMANN, E. Security governance and the private military industry in Europe and North America: Analysis. **Conflict, Security & Development,** v. 5, n. 2, p. 247-268, 2005.

KUEHL, D. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin D.; STARR, Stuart S.; WENTZ Larry K.. (Eds.). **Cyberpower and National Security.** University of Nebraska Press. 2009

LAYNE, C. The unipolar illusion: Why new great powers will rise. **International security,** v. 17, n. 4, p. 5-51, 1993.

LERNER, K. L. The British Intelligence Community: Secret Intelligence Service (MI6), Security Service (MI5), Government Communications Headquarters (GCHQ) and other entities. **Government Information Quarterly. Elsevier, 2005. Draft COPY Originally published in Lerner, K. Lee and B. Wilmoth Lerner, Encyclopedia of Espionage, Intelligence, and Security, Thomson Gale**, 2004.

LEWIS, J. Cybersecurity and critical infrastructure protection. **Center for Strategic and International Studies**, v. 9, 2006.

LIBICKI, M. C. Cyberdeterrence and cyberwar. Rand Corporation, 2009

LOBATO, L. C.; KENKEL, K. M. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional,** v. 58, n. 2, p. 23-43, 2015.

LOPEZ-LUCIA, E. Regional powers and regional security governance: An interpretive perspective on the policies of Nigeria and Brazil. **International Relations,** v. 29, n. 3, p. 348-362, 2015.

LUKASIK, S. Why the ARPANET was built. **IEEE Annals of the History of Computing**, v. 33, n. 3, p. 4-21, 2010.

MAZIERO, A. C.; AYRES PINTO, D. J. **Poder cibernético e o espaço internacional**: uma perspectiva a partir das Teorias das Relações Internacionais. 7º Encontro Nacional da Associação Brasileira de Relações Internacionais. 2019.

MEARSHEIMER, J. J. et al. **The tragedy of great power politics.** WW Norton & Company, 2001.

MEDEIROS, B. P. **Ciberespaço e Relações Internacionais: Rumo a Construção de um novo Paradigma?** (Dissertação de Mestrado). Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, RJ, 2019.

MEDEIROS, B. P.; GOLDONI, L. R. F. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional,** v. 42, n. 1, p. 31-54, 2020.

MEDEIROS FILHO, O. Em busca de ordem cibernética internacional. **Segurança e Defesa Cibernética: da fronteira física aos muros virtuais,** 2014.

MELLO, G. R.; SLOMSKI, V. Índice de governança eletrônica dos estados Brasileiros (2009): no âmbito do poder executivo. **JISTEM-Journal of Information Systems and Technology Management**, v. 7, n. 2, p. 375-408, 2010.

MORGENTHAU, H. J. **A política entre as nações:** a luta pelo poder e pela paz. Brasília: Editora da UnB, 2003.

MOSTAFAVI, M. **Human Security Unit,** OCHA at the CMC Finland organized Human Security Training on 21 April, 2009, Tuusula, Finland.

NEUMAN, D. Qualitative research in educational communications and technology: A brief introduction to principles and procedures. **Journal of Computing in Higher Education,** v. 26, n. 1, p. 69-86, 2014.

NIELSEN, S. C. Pursuing security in cyberspace: Strategic and organizational challenges. **Orbis,** v. 56, n. 3, p. 336-356, 2012.

NOLTE, D. **How to compare regional powers:** analytical concepts and research topics. **Review of international studies**, p. 881-901, 2010.

NOY, C. Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. I**nternational Journal of social research methodology,** v. 11, n. 4, p. 327-344, 2008.

NYE, J. S. The future of power. Public Affairs, 2011.

OLIVEIRA, A. M.; ROCHA, H. R.; BOSSO, J. P. C. **As capacidades de defesa e segurança cibernética de Brasil e Israel: uma análise comparada.** Disponível em: https://www.ufsm.br/app/uploads/sites/372/2019/05/Ebook-Anais-do-X-EERRI-.pdf. Acesso em: 01 mar. 2021.

OLIVEIRA, A. G.; PISA, B. J. **IGovP:** índice de avaliação da governança pública — instrumento de planejamento do Estado e de controle social pelo cidadão. Revista de Administração Pública (RAP). 2015.

PAGLIARI, G. C.; AYRES PINTO, D. J.; BARROSO, J. L. V. Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: um estudo prospectivo. In: Marcos Guedes de Oliveira. (Org.). **Defesa Cibernética e Mobilização Nacional.** 1ed.Recife: UFPE, 2020, v. 1, p. 153-174.

PARKER, D. The state of security in cyberspace. **Computer Fraud & Security Bulletin,** v. 1993, n. 8, p. 15-18, 1993.

PETERS, B. G.; PIERRE, J. Governance without government? Rethinking public administration. **Journal of public administration research and theory**, v. 8, n. 2, p. 223-243, 1998.

PETERS, M. et al. Research into headache: the contribution of qualitative methods. **Headache: The Journal of Head and Face Pain,** v. 42, n. 10, p. 1051-1059, 2002.

PHILLIPS, J. Exploring the citizen-driven response to crisis in cyberspace, risk and the need for resilience. In: **2015 IEEE Canada International Humanitarian Technology Conference (IHTC2015)**. IEEE, 2015. p. 1-6.

PODUVAL, S. Contours of security in cyberspace. **Maritime Affairs: Journal of the National Maritime Foundation of India,** v. 8, n. 2, p. 73-94, 2012.

PORTELA, L. S. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. **Revista Brasileira de Estudos de Defesa,** v. 5, n. 1, 2018.

PRODANOV, C. C.; DE FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição.** Editora Feevale, 2013.

RANTAPELKONEN, J. et al. The fog of cyber defence. **Julkaisusarja 2. Artikkelikokoelma n: o 10,** 2013.

RATTRAY, G. J. An environmental approach to understanding cyberpower. **Cyberpower and National Security**, p. 253-274, 2009.

RID, T.; BUCHANAN, B. Attributing cyber attacks. **Journal of Strategic Studies**, v. 38, n. 1-2, p. 4-37, 2015.

ROCHA, H. R. et al**. Estratégias de defesa e segurança cibernética de Argentina, Brasil e Uruguai:** uma análise comparada. 2019.

RODRIGUES, K. F. Desvelando o conceito de transparência: seus limites, suas variedades e a criação de uma tipologia. **Cadernos EBAPE. BR**, v. 18, p. 237-253, 2020.

RUDZIT, G.; NOGAMI, O. National security and defense: basic concepts for an analysis. **Revista Brasileira de Política Internacional,** v. 53, n. 1, p. 5-24, 2010.

SANTOS, A, M. Segurança e Globalização: A perspectiva dos estudos críticos de segurança. **PROELIUM**, v. 7, p. 107-114, 2016.

SANTOS, M. **A natureza do espaço: técnica e tempo, razão e emoção.** Edusp, 2002.

SCHEDLER, A.; DIAMOND, L. J.; PLATTNER, M. F. (Ed.). **The self-restraining state: power and accountability in new democracies**. Lynne Rienner Publishers, 1999.

SCHELLING, T. C. The strategy of conflict. Prospectus for a reorientation of game theory. **Journal of Conflict Resolution,** v. 2, n. 3, p. 203-264, 1958.

SCHMITT, M. N. (Ed.). **Tallinn manual on the international law applicable to cyber warfare.** Cambridge University Press, 2013.

SCHMITT, M. N. (Ed.). **Tallinn manual 2.0 on the international law applicable to cyber operations.** Cambridge University Press, 2017.

SEXTON, M. UK cybersecurity strategy and active cyber defence–issues and risks. **Journal of Cyber Policy,** v. 1, n. 2, p. 222-242, 2016.

SHELDON, J. B. Deciphering cyberpower: Strategic purpose in peace and war. **Strategic Studies Quarterly**, v. 5, n. 2, p. 95-112, 2011.

SILVEIRA, D. T.; CÓRDOVA, F. P. **A pesquisa científica.** In: GERHARDDT, T. E. e SILVEIRA, D. T. (org.). Métodos de Pesquisa. Porto Alegre: Editora de UFRGS, 2009. P. 31 -42.

SKINNER, R, J. The importance of designating cyberspace weapon systems. **AIR AND SPACE POWER JOURNAL MAXWELL AFB AL**, 2013.

SOUZA, E. A. A.; ALMEIDA, N. N. A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço político-administrativo do estado. **Revista da Escola de Guerra Naval,** v. 22, n. 2, p. 381, 2016.

SOUZA, G. L. M. **Reflexos da digitalização da Guerra na Política Internacional do Século XXI: Uma análise exploratória da securitização do Ciberespaço nos Estados Unidos, Brasil e Canadá.** 2013. Dissertação (Mestrado em Ciência Política) - Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco, Recife, 2013.

TADJBAKHSH, S; CHENOY, A. **Human security: Concepts and implications**. Routledge, 2007.

TSAGOURIAS, N. Cyber attacks, self-defence and the problem of attribution. **Journal of conflict and security law**, v. 17, n. 2, p. 229-244, 2012.

TURK, Robert J. **Cyber incidents involving control systems.** Idaho National Laboratory (INL), 2005.

ULHØI, J. P. Revisiting the principal-agent theory of agency: comments on the firm-level and cross-national embeddedness theses. **Journal of Organizational Behavior**, v. 28, n. 1, p. 75-80, 2007.

UNITED KINGDOM. **Cyber Security.** 2016. Disponível em: https://www.local.gov.uk/our-support/efficiency-and-income-generation/digital/cyber-security#:~:text=The%20National%20Cyber%20Security%20Strategy,unauthorised%20access%2C%20harm%20or%20misuse. Acesso em: 01 mar. 2021.

UNITED KINGDOM. **GCHQ is a world-leading intelligence, cyber and security agency with a mission to keep the UK safe**. 2020. Disponível em: https://www.gchq.gov.uk/section/mission/overview. Acesso em: 26 nov. 2021.

UNITED KINGDOM. **Global Britain in a Competitive Age: The Integrated Review of Security,** Defence, Development and Foreign Policy, March 2021, Command Paper 403. 2021.

UNITED KINGDOM. Her Majesty's Government. **National Cyber Security Strategy 2016-2021**.

UNITED KINGDOM. **National Cyber Force**: a defence and intelligence partnership. Disponível em:

https://www.gov.uk/government/organisations/national-cyber-force/about. Acesso em: 26 nov. 2021.

UNITED KINGDOM. **National Cyber Force Transforms country's cyber capabilities to protect UK**. Disponível em: https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk. Acesso em: 26 nov. 2021.

UNITED KINGDOM. **Secret Intelligence Service (MI6)**. Disponível em: https://www.sis.gov.uk/about-us.html. Acesso em: 26 nov. 2021.

UNITED KINGDOM. **The role of the National Cyber Security Centre (NCSC)**. Disponível em: https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/. Acesso em: 26 nov. 2021.

UNITED KINGDOM. **What is the difference between MI5 and MI6 (SIS)?** 2020. Disponível em: https://www.mi5.gov.uk/faq/what-is-the-difference-between-mi5-and-mi6-sis. Acesso em: 26 nov. 2021.

UNITED STATES. **Achieve and Maintain Cyberspace Superiority**. Command Vision for US Cyber Command. Disponível em: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf. Acesso em: 26 nov. 2021.

UNITED STATES. **Cybersecurity Glossary.** 2020. Disponível em: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary. Acesso em: 01 mar. 2021.

UNITED STATES. **CYBERSECURITY UNIT**. Disponível em: https://www.justice.gov/criminal-ccips/cybersecurity-unit. Acesso em: 26 nov. 2021.

UNITED STATES. **Department of Homeland Security**: cybersecurity and infrastructure security agency budget overview. Cybersecurity and Infrastructure Security Agency Budget Overview. Disponível em: https://www.dhs.gov/sites/default/files/publications/cybersecurity_and_infrastructure_security_agency.pdf. Acesso em: 26 nov. 2021.

UNITED STATES. **DOD Dictionary of Military and Associated Terms.** 2021.

UNITED STATES. **National Defense Strategy of The United States of America**. 2018.

UNITED STATES. **NSA Cybersecurity Overview**. 2020. Disponível em: https://www.nsa.gov/Cybersecurity/Overview/. Acesso em: 26 nov. 2021.

UNITED STATES. **Secure Cyberspace and Critical Infrastructure**. Disponível em: https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure. Acesso em: 26 nov. 2021.

UNITED STATES. **SECURING FEDERAL NETWORKS**. Disponível em: https://www.cisa.gov/securing-federal-networks. Acesso em: 26 nov. 2021.

UNITED STATES. **The Cyber Threat**. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 26 nov. 2021.

UNITED STATES. **The National Strategy to Secure Cyberspace.** Washington, DC: The White House, February. 2003.

UNITED STATES. **United States Secret Service**. Disponível em: https://www.secretservice.gov/investigation. Acesso em: 26 nov. 2021.

UNITED STATES. **United States Secret Service**: cyber investigations. Cyber Investigations. Disponível em: https://www.secretservice.gov/investigation/cyber. Acesso em: 26 nov. 2021.

UNITED STATES. **What is the FBI?** Disponível em: https://www.fbi.gov/about/faqs/what-is-the-fbi. Acesso em: 26 nov. 2021.

VENTRE, D. Ciberguerra. In: Academia General Militar. **Seguridad Global y Potencias Emergentes en un Mundo Multipolar.** XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza. 2012.

VILLA, R. D. Security Community or Balance of Power? Hybrid Security Governance in Latin America. In: **Power Dynamics and Regional Security in Latin America.** Palgrave Macmillan, London, 2017. p. 77-99.

VOO, J. et al. National Cyber Power Index 2020. **Belfer Center for Science and International Affairs, Harvard Kennedy School**, 2020.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security,** v. 38, p. 97-102, 2013.

YONG, G.; WENHAO, C. Developing a city governance index: based on surveys in five major Chinese cities. Social indicators research, v. 109, n. 2, p. 305-316, 2012.

YOULD, R. Beyond the American fortress: Understanding homeland security in the information age. Bombs and bandwidth: **The emerging relationship between information technology and security,** p. 74-97, 2003.

WALDEN, I. Crime and security in Cyberspace. **Cambridge Review of International Affairs,** v. 18, n. 1, p. 51-68, 2005.

WALTZ, K. N. et al. **Theory of international politics.** 1979.

WARREN, M, E. Max Weber's Nietzschean conception of power. **History of The Human Sciences**, v. 5, n. 3, p. 19-37, 1992.

WEBER, M. Economy and society: An outline of interpretive sociology. **Univ of California Press,** 1978.

WEBBER, M. et al. The governance of European security. **Review of international studies,** p. 3-26, 2004.

WILLETT, M. Assessing Cyber Power. **Survival,** v. 61, n. 1, p. 85-90, 2019.

WINTER, L, M. A concepção de Estado e de poder político em Maquiavel. **Tempo da Ciência**, v. 13, n. 25, p. 117-128, 2006.

WIRTZ, J. J. Life in the “Gray Zone”: observations for contemporary strategists. **Defense & Security Analysis**, v. 33, n. 2, p. 106-114, 2017.

WOHLFORTH, W. C. The stability of a unipolar world. **International security,** v. 24, n. 1, p. 5-41, 1999.

WOHLFORTH, W. C. Status dilemmas and inter-state conflict. **Status and World Order, TV Paul, Deborah Larson, and William C. Wohlforth, eds., Forthcoming,** 2012.

WOLFERS, A. National Security as an ambiguous symbol. **Political science quarterly**, v. 67, n. 4, p. 481-502, 1952.

WOODBURN, C. M. **Leader Development of Cyber Soldiers through Mission Command**. 2012. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA591139.pdf. Acesso em: 26 nov. 2021.